D-Link®
Building Networks for People

XSTACK®

User Manual

Product Model: DES-3200-10/18/28/28F

Layer 2 Managed Ethernet Switch

Release 1.1

Information in this document is subject to change without notice.

© 2009 D-Link Corporation. All rights reserved.

Reproduction in any manner whatsoever without the written permission of D-Link Corporation is strictly forbidden.

Trademarks used in this text: D-Link and the D-LINK logo are trademarks of D-Link Corporation; Microsoft and Windows are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. D-Link Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

August 2009 P/N 651S3200.015G

Table of Contents

Intended Readers viii
Typographical Conventions viii
Notes, Notices, and Cautions viii
Web-based Switch Configuration 9
Introduction 9
Login to Web Manager 9
Web-based User Interface 10
Web Pages 11
Configuration 12
Device Information 13
System Information 13
Serial Port Settings 14
IP Address Settings 14
IPv6 Address Settings 16
IPv6 Route Settings 17
IPv6 Neighbor Settings 17
Port Configuration 18
Port Settings 18
Port Description Settings 20
Port Error Disabled 20
Static ARP Settings 21
User Accounts 22
System Log Configuration 23
System Log Settings 23
System Log Server 23
DHCP Relay 25
DHCP Relay Global Settings 25
DHCP Relay Interface Settings 28
DHCP Local Relay Settings 28
DHCP Auto Configuration Settings 29
MAC Address Aging Time 29
Web Settings 29
Telnet Settings 30
Password Encryption 30
CLI Paging Settings 30
Firmware Information 31
SNTP Settings 32
Time Settings 32
Time Zone Settings 33

SMTP Settings 35
SMTP Service Settings 35
SMTP Service 36
MAC Notification Settings 36
MAC Notification Global Settings 36
MAC Notification Port Settings 36
SNMP Settings 37
SNMP View Table 38
SNMP Group Table 39
SNMP User Table 40
SNMP Community Table 41
SNMP Host Table 42
SNMP Engine ID 42
SNMP Trap Configuration 43
RMON 43
Time Range Settings 44
Single IP Management 44
Single IP Settings 46
Topology 47
Tool Tips 49
Right-Click 50
Menu Bar 52
Firmware Upgrade 53
Configuration File Backup/Restore 53
Upload Log File 54
Gratuitous ARP 54
Gratuitous ARP Global Settings 54
Gratuitous ARP Settings 55
ARP Spoofing Prevention Settings 56
L2 Features 57
Jumbo Frame 57
VLANs 58
Understanding IEEE 802.1p Priority 58
VLAN Description 58
IEEE 802.1Q VLANs 59
Q-in-Q VLANs 62
802.1Q Static VLAN 64
Q-in-Q 67
Q-in-Q Settings 68
VLAN Translation Settings 69
802.1v Protocol VLAN 69
802.1v Protocol Group Settings 69
802.1v Protocol VLAN Settings 70

VLAN Trunk Settings 71
GVRP Settings 72
Asymmetric VLAN Settings 73
MAC-based VLAN Settings 73
PVID Auto Assign Settings 74
Port Trunking 74
LACP Port Settings 76
Traffic Segmentation 77
BPDU Tunneling Settings 78
IGMP Snooping 78
IGMP Snooping Settings 78
IGMP Access Control Settings 80
IGMP Snooping Multicast VLAN Settings 81
IP Multicast Profile Settings 82
Limited Multicast Range Settings 84
Max Multicast Group Settings 84
MLD Snooping Settings 85
Port Mirror 88
Loopback Detection Settings 89
Spanning Tree 90
STP Bridge Global Settings 92
STP Port Settings 93
MST Configuration Identification 95
STP Instance Settings 96
MSTP Port Information 97
Forwarding & Filtering 97
Unicast Forwarding Settings 97
Multicast Forwarding Settings 98
Multicast Filtering Mode 99
LLDP 99
LLDP Global Settings 100
LLDP Port Settings 101
LLDP Basic TLVs Settings 102
LLDP Dot1 TLVs Settings 103
LLDP Dot3 TLVs Settings 104
QoS 105
Advantages of QoS 105
Understanding QoS 106
Bandwidth Control 107
Traffic Control 107
802.1p Default Priority 110
802.1p User Priority 110
QoS Scheduling Settings 111

Priority Mapping 112
TOS Mapping 113
DSCP Mapping 114
Security 115
Safeguard Engine 115
Trusted Host 117
IP-MAC-Port Binding 117
IMP Binding Global Settings 117
IMP Binding Port Settings 118
IMP Binding Entry Settings 119
DHCP Snooping Entries 120
MAC Block List 120
Port Security 120
Port Security Port Settings 120
Port Security FDB Entries 122
802.1X 122
Understanding 802.1X Port-based and MAC-based Network Access Control 125
Port-Based Network Access Control 125
MAC-Based Network Access Control 126
802.1X Settings 127
802.1X User 128
Authentication RADIUS Server 129
Guest VLAN Configuration 130
Guest VLAN 131
Initialize Port(s) 131
Reauthenticate Port(s) 132
SSL Settings 133
Download Certificate 134
Ciphersuite 134
SSH 135
SSH Settings 136
SSH Authmode and Algorithm Settings 136
SSH User Authentication Lists 138
Access Authentication Control 139
Authentication Policy Settings 140
Application Authentication Settings 140
Authentication Server Group 141
Authentication Server 142
Login Method Lists 143
Enable Method Lists 144
Local Enable Password Settings 145
MAC-based Access Control 146
MAC-based Access Control Settings 146

MAC-based Access Control Local Settings 148
DoS Prevention Settings 149
ACL 150
ACL Configuration Wizard 150
Access Profile List 151
CPU Interface Filtering 168
CPU Access Profile List 168
ACL Finder 182
ACL Flow Meter 182
Monitoring 184
Cable Diagnostic 184
CPU Utilization 184
Port Utilization 185
Packet Size 186
Memory Utilization 188
Packets 188
Received (Rx) 188
UMB_cast (Rx) 190
Transmitted (Tx) 191
Errors 193
Received (RX) 193
Transmitted (TX) 195
Port Access Control 196
RADIUS Authentication 197
RADIUS Account Client 198
Authenticator State 200
Authenticator Statistics 201
Authenticator Session Statistics 202
Authenticator Diagnostics 204
Browse ARP Table 206
Browse VLAN 206
IGMP Snooping 206
Browse IGMP Router Port 206
IGMP Snooping Group 207
IGMP Snooping Host 208
MLD Snooping 208
Browse MLD Router Port 208
MLD Snooping Group 209
LLDP 209
LLDP Statistics System 209
LLDP Local Port Information 210
LLDP Remote Port Information 210
MBA Authentication State 211

Browse Session Table 211
MAC Address Table 211
System Log 212
Save and Tools 213
Save Configuration 213
Save Log 214
Save All 214
Configuration File Upload & Download 214
Upload Log File 215
Reset 215
Ping Test 216
Download Firmware 217
Reboot System 217
Mitigating ARP Spoofing Attacks Using Packet Content ACL 218
System Log Entries 226
Glossary 237

Intended Readers

The ***DES-3200-10/18/28/28F User Manual*** contains information for setup and management of the Switch. This manual is intended for network managers familiar with network management concepts and terminology.

Typographical Conventions

Convention	Description
[ ]	In a command line, square brackets indicate an optional entry. For example: [copy filename] means that optionally you can type copy followed by the name of the file. Do not type the brackets.
Bold font	Indicates a button, a toolbar icon, menu, or menu item. For example: Open the **File** menu and choose **Cancel**. Used for emphasis. May also indicate system messages or prompts appearing on your screen. For example: You have mail. Bold font is also used to represent filenames, program names and commands. For example: use the copy command.
Boldface Typewriter Font	Indicates commands and responses to prompts that must be typed exactly as printed in the manual.
Initial capital letter	Indicates a window name. Names of keys on the keyboard have initial capitals. For example: Click Enter.
Italics	Indicates a window name or a field. Also can indicate a variables or parameter that is replaced with an appropriate word or string. For example: type filename means that you should type the actual filename instead of the word shown in italic.
Menu Name > Menu Option	**Menu Name > Menu Option** Indicates the menu structure. **Device > Port > Port Properties** means the Port Properties menu option under the Port menu option that is located under the Device menu.

Notes, Notices, and Cautions

A **NOTE** indicates important information that helps you make better use of your device.

A **NOTICE** indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

A **CAUTION** indicates a potential for property damage, personal injury, or death.

Section 1

Web-based Switch Configuration

Introduction

Login to Web Manager

Web-based User Interface

Web Pages

Introduction

All software functions of the Switch can be managed, configured and monitored via the embedded web-based (HTML) interface. The Switch can be managed from remote stations anywhere on the network through a standard browser such as Firefox, Microsoft Internet Explorer, Mozilla, or Netscape. The browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol.

The Web-based management module and the Console program (and Telnet) are different ways to access the same internal switching software and configure it. Thus, all settings encountered in Web-based management are the same as those found in the console program.

Login to Web Manager

To begin managing the Switch, simply run the browser you have installed on your computer and point it to the IP address you have defined for the device. The URL in the address bar should read something like: http://123.123.123.123, where the numbers 123 represent the IP address of the Switch.

NOTE: The Factory default IP address for the Switch is 10.90.90.90.

This opens the management module's user authentication window, as seen below.

Figure 1 - 1 Enter Network Password dialog

Enter “admin” in both the User Name and Password fields and click **OK**. This will open the Web-based user interface. The Switch management features available in the web-based manager are explained below.

Web-based User Interface

The user interface provides access to various Switch configuration and management windows, allows you to view performance statistics, and permits you to graphically monitor the system status.

Areas of the User Interface

The figure below shows the user interface. The user interface is divided into three distinct areas as described in the table.

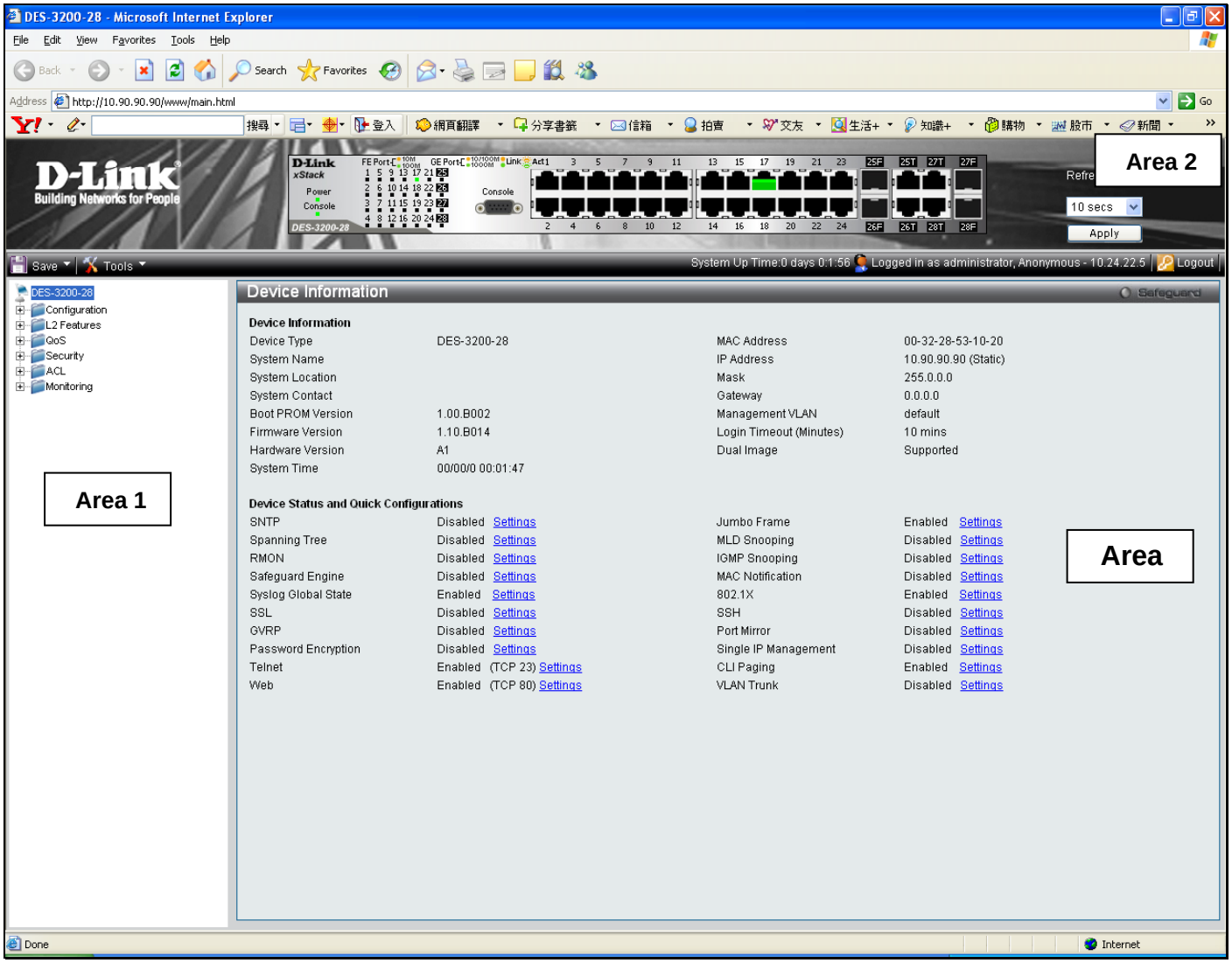


Figure 1 - 2 Main Web-Manager page

Area	Function
Area 1	Select the folder or window to be displayed. The folder icons can be opened to display the hyperlinked window buttons and subfolders contained within them. Click the D-Link logo to go to the D-Link website.
Area 2	Presents a graphical near real-time image of the front panel of the Switch. This area displays the Switch's ports and expansion modules, showing port activity, duplex mode, or flow control, depending on the specified mode. Various areas of the graphic can be selected for performing management functions, including port configuration.
Area 3	Presents switch information based on your selection and the entry of configuration data.

NOTICE: Any changes made to the Switch configuration during the current session must be saved in the **Save Configuration** window (**Save > Save Configuration**) or use the command line interface (CLI) command **save config**.

Web Pages

When you connect to the management mode of the Switch with a Web browser, a login window is displayed. Enter a user name and password to access the Switch's management mode.

Below is a list and description of the main folders available in the Web interface:

Configuration – Contains main windows concerning Device Information, System Information, Serial Port Settings, IP Address, IPv6 Interface Settings, IPv6 Route Settings, IPv6 Neighbor Settings, Port Configuration, Static ARP Settings, User Accounts, System Log Configuration, DHCP Relay, DHCP Auto Configuration Settings, MAC Address Aging Time, Web Settings, Telnet Settings, Password Encryption, CLI Paging Settings, Firmware Information, SNTP Settings, SMTP Settings, MAC Notification Settings, SNMP Settings, Time Range Settings, Single IP Management, Gratuitous ARP, and ARP Spoofing Prevention Settings.

L2 Features – Contains main windows concerning Jumbo Frame, 802.1Q Static VLAN, Q-in-Q, 802.1v Protocol VLAN, VLAN Trunk Settings, GVRP Settings, Asymmetric VLAN Settings, MAC-based VLAN Settings, PVID Auto Assign Settings, Port Trunking, LACP Port Settings, Traffic Segmentation, BPDU Tunneling Settings, IGMP Snooping, MLD Snooping Settings, Port Mirror, Loopback Detection Settings, Spanning Tree, Forwarding & Filtering, and LLDP.

QoS – Contains main windows concerning Bandwidth Control, Traffic Control, 802.1P Default Priority, 802.1P User Priority, QoS Scheduling Settings, Priority Mapping, TOS Mapping, and DSCP Mapping.

Security – Contains main windows concerning Safeguard Engine, Trusted Host, IP-MAC-Port Binding, Port Security, 802.1X, SSL Settings, SSH, Access Authentication Control, MAC-based Access Control, and DoS Prevention Settings.

ACL – Contains main windows concerning ACL Configuration Wizard, Access Profile List, CPU Access Profile List, ACL Finder, and ACL Flow Meter.

Monitoring – Contains main windows concerning Cable Diagnostic, CPU Utilization, Port Utilization, Packet Size, Memory Utilization, Packets, Errors, Port Access Control, Browse ARP Table, Browse VLAN, IGMP Snooping, MLD Snooping, LLDP, MBA Authentication State, Browse Session Table, MAC Address Table, and System Log.

Save & Tools – Contains main windows concerning Save Configuration, Save Log, Save All, Configuration File Upload & Download, Upload Log File, Reset, Ping Test, Download Firmware, and Reboot System.

NOTE: Be sure to configure the user name and password in the **User Accounts** window (**Configuration > User Accounts**) before connecting the Switch to the greater network.

Section 2

Configuration

Device Information
System Information
Serial Port Settings
IP Address Settings
IPv6 Interface Settings
IPv6 Route Settings
IPv6 Neighbor Settings
Port Configuration
Static ARP Settings
User Accounts
System Log Configuration
DHCP Relay
DHCP Auto Configuration Settings
MAC Address Aging Time
Web Settings
Telnet Settings
Password Encryption
CLI Paging Settings
Firmware Information
SNTP Settings
SMTP Settings
MAC Notification Settings
SNMP Settings
Time Range Settings
Single IP Management
Gratuitous ARP
ARP Spoofing Prevention Settings

Device Information

This window contains the main settings for all major functions on the Switch and appears automatically when you log on. To return to the **Device Information** window, click the **DES-3200-10/18/28/28F** folder. The **Device Information** window shows the Switch's MAC Address (assigned by the factory and unchangeable), the Boot PROM Version, Firmware Version, the Hardware Version, and other information about different settings on the Switch. This information is helpful to keep track of PROM and firmware updates and to obtain the Switch's MAC address for entry into another network device's address table, if necessary. In addition, this window displays the status of functions on the Switch to quickly assess their current global status. Some functions are hyper-linked to their configuration window for easy access from the **Device Information** window.

Figure 2 - 1. Device Information window

System Information

This window contains the System Information details. The user may enter a System Name, System Location and System Contact to aid in defining the Switch, to the user's preference. This window displays the MAC Address, Firmware Version and Hardware Version.

Click **Configuration > System Information** to display the following window:

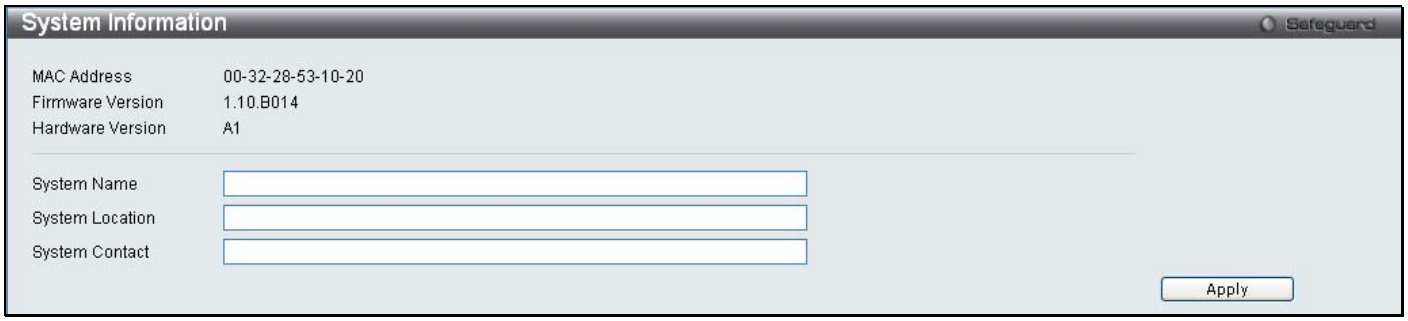


Figure 2 - 2. System Information window

The fields that can be configured are described below:

Parameter	Description
System Name	Enter a system name for the Switch, if so desired. This name will identify it in the Switch network.
System Location	Enter the location of the Switch, if so desired.
System Contact	Enter a contact name for the Switch, if so desired.

Click **Apply** to implement changes made.

Serial Port Settings

The following window allows the Baud Rate and the Auto Logout to be changed as well as containing information about the Serial Port Settings.

Click **Configuration > Serial Port Settings** to display this window:

Figure 2 - 3. Serial Port Settings window

Parameter	Description
Baud Rate	This field specifies the baud rate for the serial port on the Switch. There are four possible baud rates to choose from, *9600*, *19200*, *38400* and *115200.* For a connection to the Switch using the CLI interface, the baud rate must be set to *9600*, which is the default setting.
Auto Logout	Select the logout time used for the console interface. This automatically logs the user out after an idle period of time, as defined. Choose from the following options: *2 Minutes, 5 Minutes, 10 Minutes, 15 Minutes* or *Never*. The default setting is *10 minutes*.

Click **Apply** to implement changes made.

NOTE: If a user configures the serial port's baud rate, the baud rate will take effect and save immediately.

IP Address Settings

The IP address may initially be set using the console interface prior to connecting to it through the Ethernet. If the Switch IP address has not yet been changed, read the introduction of the *DES-3200-10/18/28/28F CLI Reference Manual* for more information.

Click **Configuration > IP Address Settings** to display the following window:

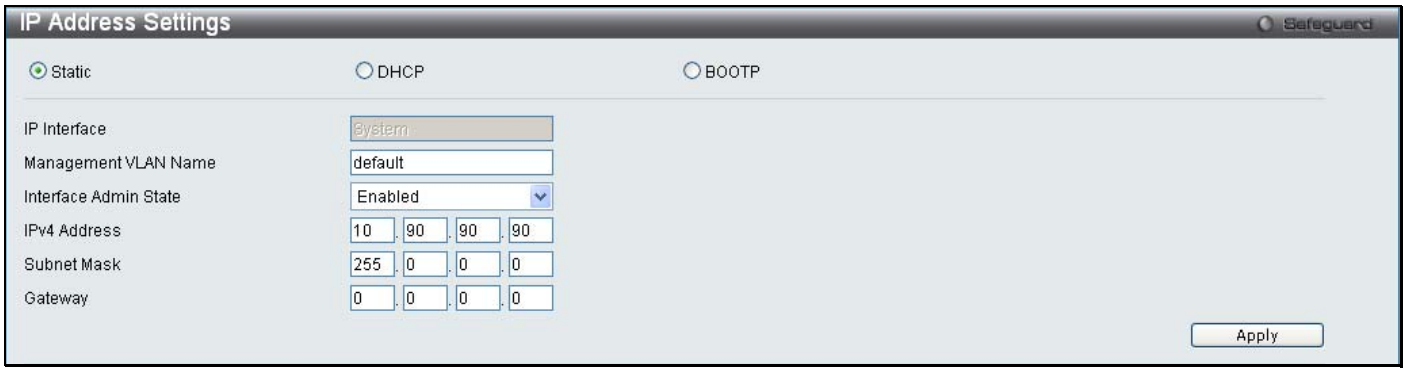


Figure 2 - 4. IP Address Settings window

To manually assign the Switch's IP address, subnet mask, and default gateway address:

1. Click *Static* at the top of the window.
2. Enter the appropriate IPv4 Address and Subnet Mask.
3. To access the Switch from a different subnet from the one it is installed on, enter the IP address of the Gateway. If the Switch will be managed from the subnet on which it is installed, leave the default address (0.0.0.0) in this field.

4. If no VLANs have been previously configured on the Switch, you can use the *default* Management VLAN Name. The *default* VLAN contains all of the Switch ports as members. If VLANs have been previously configured on the Switch, the Management VLAN Name of the VLAN that contains the port connected to the management station will have to be entered to access the Switch.
5. Use the drop-down Interface Admin State menu to select *Enabled* if it has not already been done.

NOTE: The Switch's factory default IP address is 10.90.90.90 with a subnet mask of 255.0.0.0 and a default gateway of 0.0.0.0.

To use the BOOTP or DHCP protocols to assign the Switch an IP address, subnet mask, and default gateway address, select either *BOOTP* or *DHCP*.

The IP Address Settings options are:

Parameter	Description
Static	Allows the entry of an IPv4 address, Subnet Mask, and a Default Gateway for the Switch. These fields should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal form) between 0 and 255. This address should be a unique address on the network assigned for use by the network administrator.
DHCP	The Switch will send out a DHCP broadcast request when it is powered up. The DHCP protocol allows IP addresses, network masks, and default gateways to be assigned by a DHCP server. If this option is set, the Switch will first look for a DHCP server to provide it with this information before using the default or previously entered settings.
BOOTP	The Switch will send out a BOOTP broadcast request when it is powered up. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server. If this option is set, the Switch will first look for a BOOTP server to provide it with this information before using the default or previously entered settings.
IP Interface	The current IP Interface being assigned an IP address on this window.
Management VLAN Name	This allows the entry of a VLAN Name from which a management station will be allowed to manage the Switch using TCP/IP (in-band via web manager or Telnet). Management stations that are on VLANs other than the one entered here will not be able to manage the Switch in-band unless their IP addresses are entered in the **Security IP Management** window. If VLANs have not yet been configured for the Switch, the default VLAN contains all of the Switch's ports. There are no entries in the Security IP Management table, by default, so any management station that can connect to the Switch can access the Switch until a management VLAN is specified or Management Station IP Addresses are assigned.
Interface Admin State	Toggle between *Enabled* and *Disabled*. This must be set to *Enabled* when setting an IP address on this window.
IPv4 Address	Enter the desired IPv4 address to be set. The default address is *10.90.90.90*.
Subnet Mask	A Bitmask that determines the extent of the subnet that the Switch is on. Should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed.
Gateway	IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field unchanged.

Click **Apply** to allow changes to take effect.

Setting the Switch's IP Address using the Console Interface

Each Switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application (for example BOOTP, TFTP). The Switch's default IP address is 10.90.90.90. You can change the default Switch IP address to meet the specification of your networking address scheme.

The IP address for the Switch must be set before it can be managed with the Web-based manager. The Switch IP address can be automatically set using BOOTP or DHCP protocols, in which case the actual address assigned to the Switch must be known. The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows:

Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/ yyy.yyy.yyy.yyy.** Where the x's represent the IP address to be assigned to the IP interface named System and the y's represent the corresponding subnet mask.

Alternatively, you can enter **config ipif System ipaddress xxx.xxx.xxx.xxx/z.** Where the x's represent the IP address to be assigned to the IP interface named **System** and the z represents the corresponding number of subnets in CIDR notation.

The IP interface named System on the Switch can be assigned an IP address and subnet mask which can then be used to connect a management station to the Switch's Telnet or Web-based management agent.

The system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet and the CLI or via the Web-based management agent using the above IP address to connect to the Switch.

IPv6 Address Settings

Users can display the Switch's current IPv6 interface settings.

To view the following window, click **Configuration** > **IPv6 Interface Settings**:

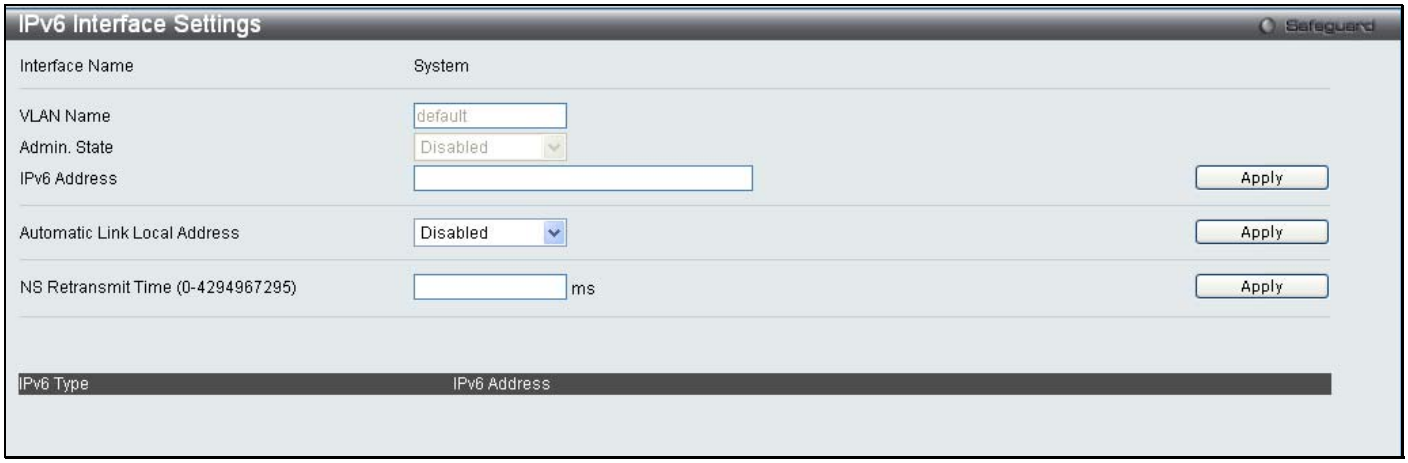


Figure 2 - 5. IPv6 Interface Settings window

To configure IPv6 interface settings, enter an IPv6 Address and click **Apply**. The new entry will appear in the table at the bottom of the window.

After making the desired changes, click the **Apply** button.

The following parameters may be configured or viewed:

Parameter	Description
Interface Name	The name of the IPv6 interface being displayed or modified.
VLAN Name	Display the VLAN name of the IPv6 interface.
Admin. State	Display the current administrator state.
IPv6 Address	Enter the IPv6 address of the interface to be modified.
Automatic Link Local Address	Toggle between *Enabled* and *Disabled*. Enabling this is helpful when no external source of network addressing information is available.
NS Retransmit Time (0-4294967295)	Enter a value between *0* and *4294967295*. This is the neighbor solicitation's retransmit timer in milliseconds. The default is zero.

IPv6 Route Settings

The user can configure the Switch's IPv6 Route Table.

To view the following window, click **Configuration** > **IPv6 Route Settings**:

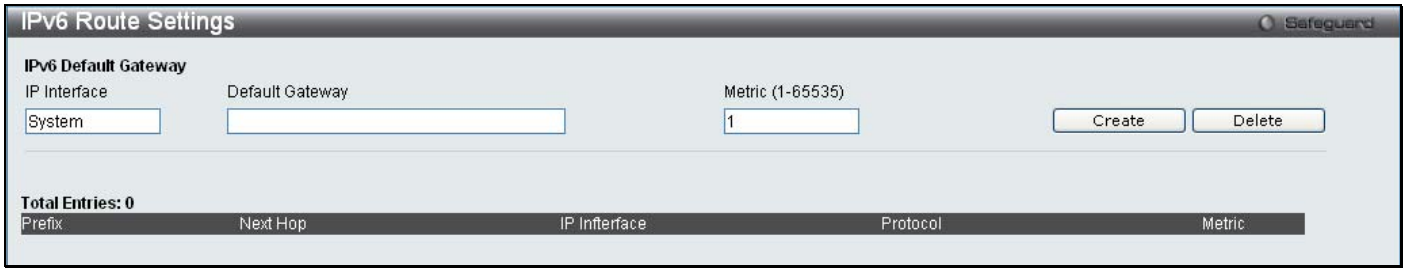


Figure 2 - 6. IPv6 Route Settings window

Enter an IP Interface, an IPv6 address in the Default Gateway field and then click the **Create** button. In addition, the Metric can be entered between *1* and *65535*. The new IPv6 route will be displayed in the table at the bottom of the window.

IPv6 Neighbor Settings

The user can configure the Switch's IPv6 neighbor settings. The Switch's current IPv6 neighbor settings will be displayed in the table at the bottom of this window.

To view the following window, click **Configuration** > **IPv6 Neighbor Settings**:

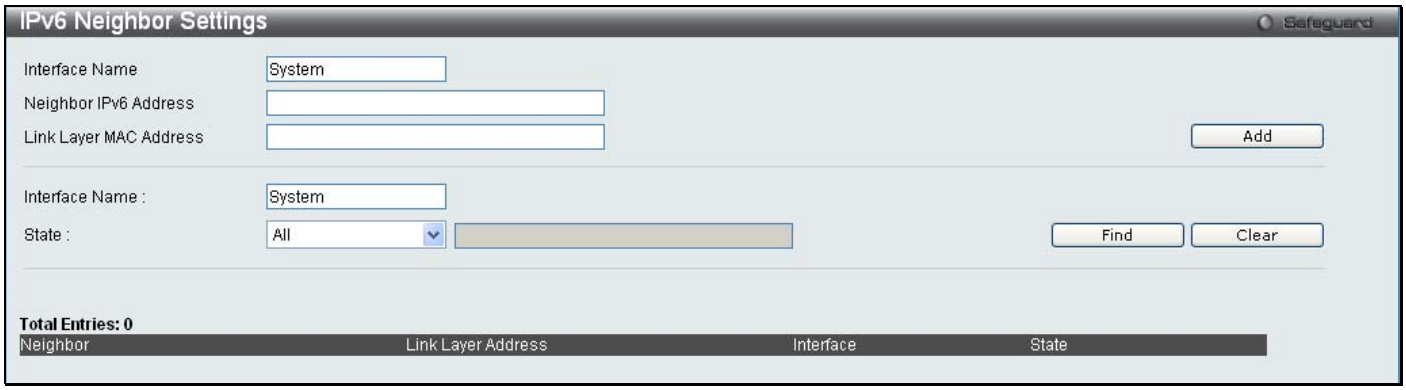


Figure 2 - 7. IPv6 Neighbor Settings window

Enter the Interface Name, Neighbor IPv6 Address, and the Link Layer MAC Address and then click the **Add** button.

To look for an IPv6 Neighbor Settings table entry, enter the Interface Name, select the desired State (*All*, *Address*, *Static*, or *Dynamic*) in the middle section of this window, and then click the **Find** button.

To delete all the entries being displayed on the table at the bottom of this window, click the **Clear** button.

The following parameters may be configured or viewed:

Parameter	Description
Interface Name	Enter the name of the IPv6 neighbor. To search for all the current interfaces on the Switch, go to the second Interface Name field in the middle part of the window, tick the All check box, and then click the **Find** button.
Neighbor IPv6 Address	Enter the neighbor IPv6 address.
Link Layer MAC Address	Enter the link layer MAC address.
State	Use the drop-down menu to select *All*, *Address*, *Static*, or *Dynamic*.

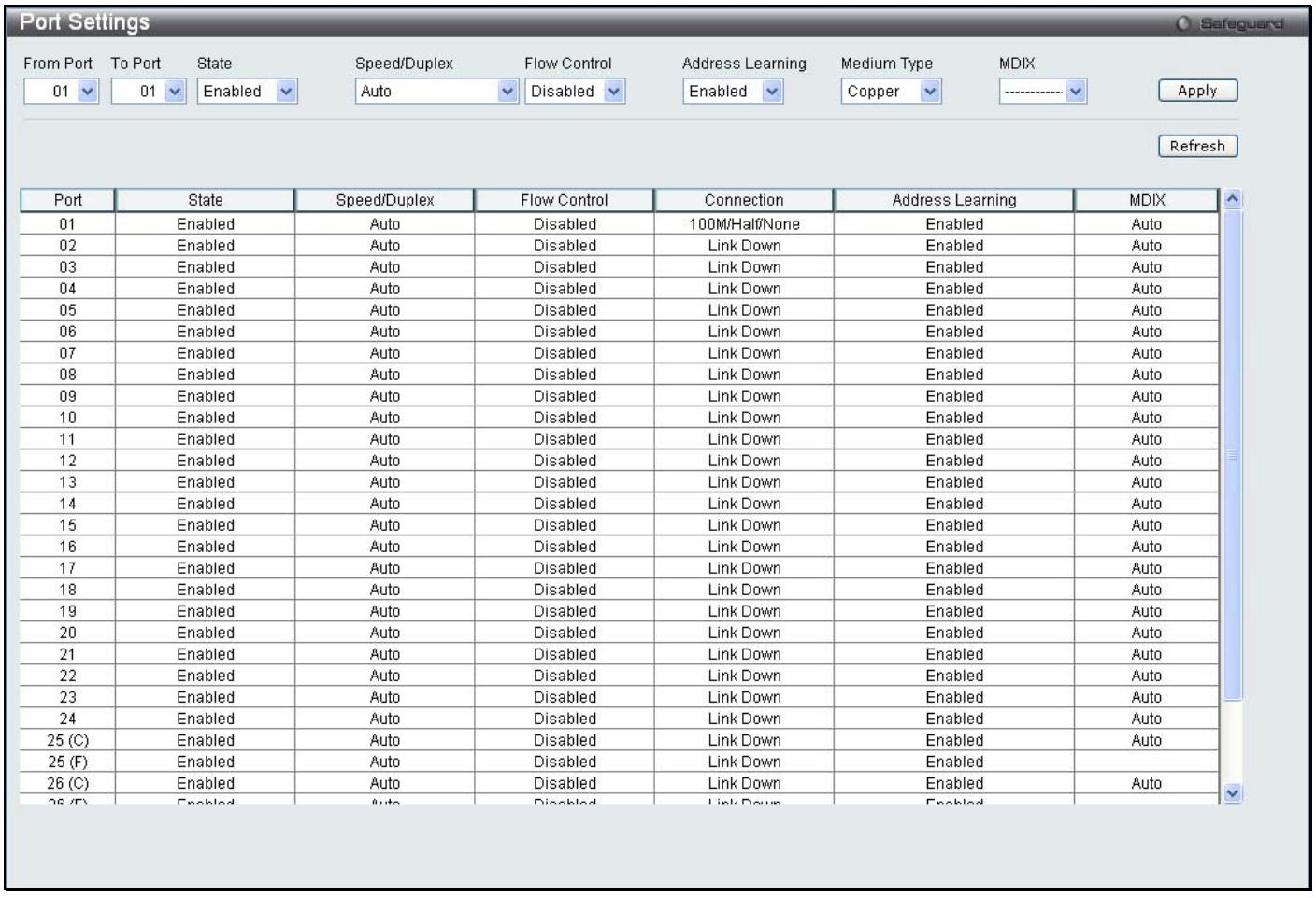
Port Configuration

This section contains information for configuring various attributes and properties for individual physical ports, including port speed and flow control.

Port Settings

Various port settings, including State, Speed/Duplex, Flow Control, Address Learnng, Medium Type, and MDIX can be configured on the Switch.

To view the following window, click **Configuration > Port Configuration > Port Settings**:


Port Settings
Safeguard
From Port
To Port
State
Speed/Duplex
Flow Control
Address Learning
Medium Type
MDIX
01
01
Enabled
Auto
Disabled
Enabled
Copper

Apply
Refresh
Port
State
Speed/Duplex
Flow Control
Connection
Address Learning
MDIX
01 Enabled Auto Disabled 100M/Half/None Enabled Auto
02 Enabled Auto Disabled Link Down Enabled Auto
03 Enabled Auto Disabled Link Down Enabled Auto
04 Enabled Auto Disabled Link Down Enabled Auto
05 Enabled Auto Disabled Link Down Enabled Auto
06 Enabled Auto Disabled Link Down Enabled Auto
07 Enabled Auto Disabled Link Down Enabled Auto
08 Enabled Auto Disabled Link Down Enabled Auto
09 Enabled Auto Disabled Link Down Enabled Auto
10 Enabled Auto Disabled Link Down Enabled Auto
11 Enabled Auto Disabled Link Down Enabled Auto
12 Enabled Auto Disabled Link Down Enabled Auto
13 Enabled Auto Disabled Link Down Enabled Auto
14 Enabled Auto Disabled Link Down Enabled Auto
15 Enabled Auto Disabled Link Down Enabled Auto
16 Enabled Auto Disabled Link Down Enabled Auto
17 Enabled Auto Disabled Link Down Enabled Auto
18 Enabled Auto Disabled Link Down Enabled Auto
19 Enabled Auto Disabled Link Down Enabled Auto
20 Enabled Auto Disabled Link Down Enabled Auto
21 Enabled Auto Disabled Link Down Enabled Auto
22 Enabled Auto Disabled Link Down Enabled Auto
23 Enabled Auto Disabled Link Down Enabled Auto
24 Enabled Auto Disabled Link Down Enabled Auto
25 (C) Enabled Auto Disabled Link Down Enabled Auto
25 (F) Enabled Auto Disabled Link Down Enabled
26 (C) Enabled Auto Disabled Link Down Enabled Auto

Figure 2 - 8. Port Settings window

To configure switch ports, choose the port or sequential range of ports using the From Port and To Port pull-down menus. Use the remaining pull-down menus to configure the parameters described below:

Parameter	Description
From Port/To Port	Use the pull-down menus to select the port or range of ports to be configured.
State	Toggle this field to either enable or disable a given port or group of ports.
Speed/Duplex	Toggle the Speed/Duplex field to either select the speed and duplex/half-duplex state of the port. *Auto* denotes auto-negotiation between 10 and 100 Mbps devices, in full- or half-duplex. The *Auto* setting allows the port to automatically determine the fastest settings the device the port is connected to can handle, and then to use those settings. The other options are *Auto*, *10M Half*, *10M Full, 100M Half* and *100M Full*, *1000M Full_Master, 1000M Full_Slave* and *1000M Full*. There is no automatic adjustment of port settings with any option other than *Auto*. The Switch allows the user to configure two types of gigabit connections; *1000M/Full_M* and *1000M/Full_S*. Gigabit connections only support full duplex connections and take on certain characteristics that are different from the other choices listed. The *1000M Full_Master* and *1000M Full_Slave* parameters refer to connections running a 1000BASE-T cable for connection between the Switch port and other device capable of a gigabit connection. The master setting (*1000M Full_Master)* will allow the port to advertise capabilities related to duplex, speed and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a master physical layer by a local source. The slave setting (*1000M Full_Slave)* uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for *1000M Full_Master*, the other side of the connection must be set for *1000M Full_Slave*. Any other configuration will result in a link down status for both ports.
Flow Control	Displays the flow control scheme used for the various port configurations. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use backpressure flow control, and *Auto* ports use an automatic selection of the two. The default is *Disabled*.
Address Learning	When *Enabled*, destination and source MAC addresses are automatically listed in the forwarding table. The default setting is *Enabled*.
Medium Type	This applies only to the Combo ports. If configuring the Combo ports this defines the type of transport medium used. SFP ports should be set at *Fiber* and the Combo 1000BASE-T ports should be set at *Copper*.
MDIX	This can be specified as *Auto*, *Normal*, or *Cross*. In *Normal* state, the port is in MDIX mode and can be connected to a PC NIC using a straight cable. If it is in *Cross* state, the port is in MDI mode, and can be connected to a port (in MDIX mode) on another switch through a straight cable.

Click **Apply** to implement the new settings on the Switch.

Port Description Settings

The Switch supports a port description feature where the user may name various ports on the Switch.

To view the following window, click **Configuration > Port Configuration > Port Description Settings**:

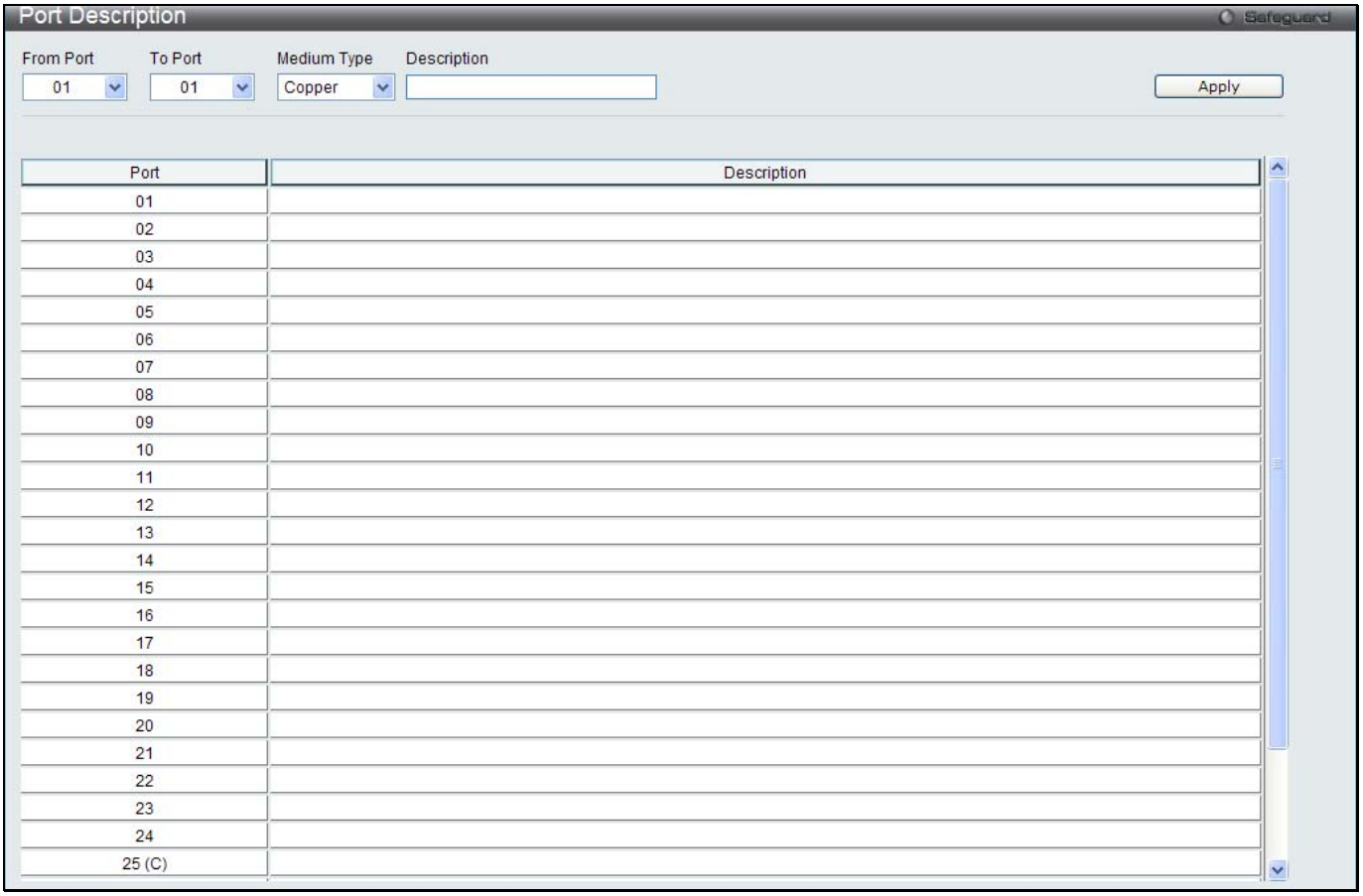


Figure 2 - 9. Port Description Settings window

Use the From Port and To Port pull-down menus to choose a port or range of ports to describe, and then enter a description of the port(s).

The Medium Type applies only to the Combo ports. If configuring the Combo ports this defines the type of transport medium used. SFP ports should be nominated *Fiber* and the Combo 1000BASE-T ports should be nominated *Copper*. The result will be displayed in the appropriate switch port number slot (C for copper ports and F for fiber ports).

The following parameters can be configured:

Parameter	Description
From Port/To Port	Use the pull-down menus to select the port or range of ports to be configured.
Medium Type	This only applies to the Combo ports. If configuring the Combo ports, this defines the type of transport medium used. SFP ports should be set at *Fiber* and the Combo 1000BASE-T ports should be set at *Copper*.
Description	The description of the the ports.

Click **Apply** to implement the new settings on the Switch.

Port Error Disabled

The following window will display information about ports that have had their connection status disabled for reasons such as STP loopback detection or link down status.

To view this window, click **Configuration > Port Configuration > Port Error Disabled**:

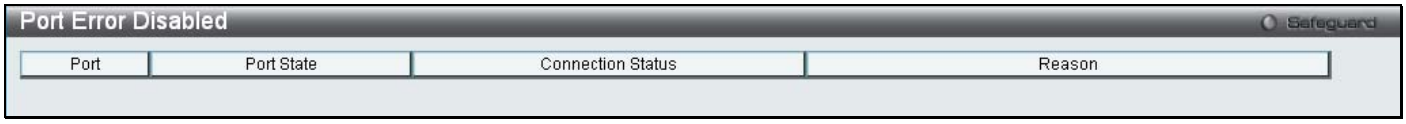


Figure 2 - 10. Port Error Disabled window

The following parameters are displayed:

Parameter	Description
Port	Displays the port that has been error disabled.
Port State	Describes the current running state of the port, whether Enabled or Disabled.
Connection Status	This field will read the uplink status of the individual ports, whether Enabled or Disabled.
Reason	Describes the reason why the port has been error-disabled, such as a STP loopback occurrence.

Static ARP Settings

The Address Resolution Protocol (ARP) is a TCP/IP protocol that converts IP addresses into physical addresses. This table allows network managers to view, define, modify and delete ARP information for specific devices. Static entries can be defined in the ARP Table. When static entries are defined, a permanent entry is entered and is used to translate IP address to MAC addresses.

To view this window, click **Configuration > Static ARP Settings**

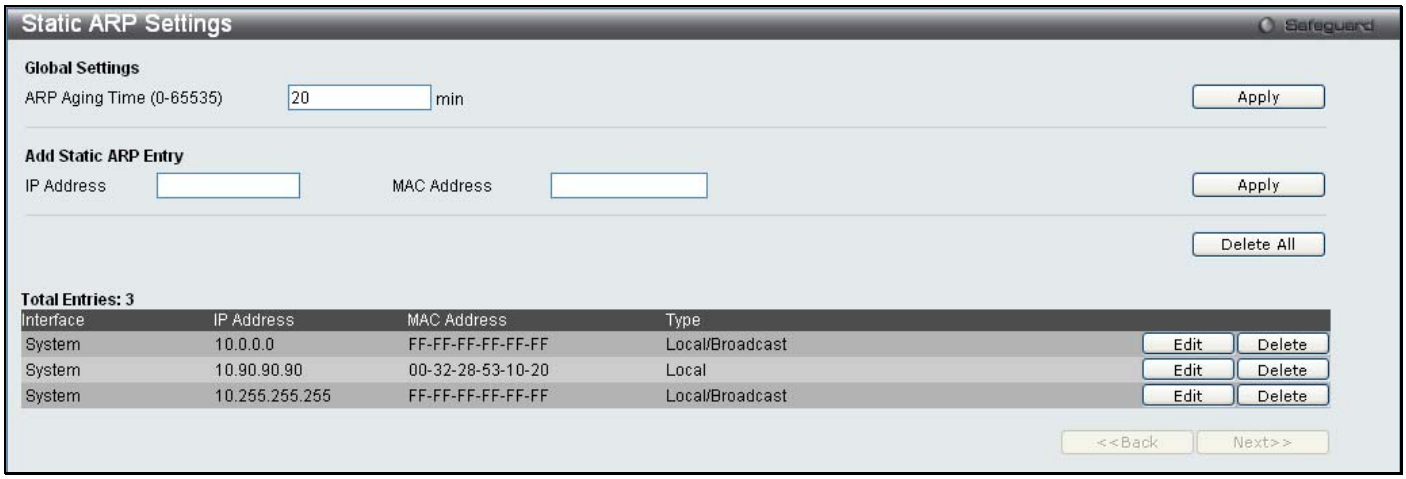


Figure 2 - 11. Static ARP Settings window

The following fields can be set:

Parameter	Description
ARP Aging Time (0-65535)	The user may globally set the maximum amount of time, in seconds, that an Address Resolution Protocol (ARP) entry can remain in the Switch's ARP table, without being accessed, before it is dropped from the table. The value may be set in the range of *0* to *65535* seconds, with a default setting of *20* seconds.
IP Address	The IP address of the ARP entry.
MAC Address	The MAC address of the ARP entry.

After entering the IP Address and MAC Address of the Static ARP entry, click **Apply** to implement the new entry. To completely clear the Static ARP Settings, click the **Delete All** button. To modify a static ARP entry, click the corresponding **Edit** button in the table. To delete a static ARP entry, click the corresponding **Delete** button in the table.

NOTE: The Switch supports up to 255 static ARP entries.

User Accounts

Use this window to control user privileges, create new users, and view existing User Accounts.

To view this window, click **Configuration > User Accounts**:

Figure 2 - 12. User Accounts window

The following fields can be set:

Parameter	Description
User Name	The name of the user, an alphanumeric string of up to 15 characters.
Password	Enter a password for the new user.
Access Right	There are two levels of user privileges, *Admin* and *User*. Some features and selections available to users with *Admin* privileges may not be available to those with *User* level privileges. (Table 2 - 1 below summarizes Admin and User level privileges)
Confirm Password	Retype the new password.

To add a new user, enter the appropriate information and click **Apply**. To modify or delete an existing user, click on the **Edit** button for that user.

NOTICE: In case of lost passwords or password corruption, please refer to the "Password Recovery Procedure" Appendix in the ***DES-3200-10/18/28/28F CLI Reference Manual*** which will guide you through the steps necessary to resolve this issue.

Admin and User Privileges

There are two levels of user privileges, **Admin** and **User**. Some menu selections available to users with **Admin** privileges may not be available to those with **User** privileges.

The following table summarizes the Admin and User privileges:

Management	Admin	User
Configuration	Yes	Read-only
Network Monitoring	Yes	Read-only
Community Strings and Trap Stations	Yes	Read-only
Update Firmware and Configuration Files	Yes	No
System Utilities	Yes	No
Factory Reset	Yes	No

User Account Management		
Add/Update/Delete User Accounts	Yes	No
View User Accounts	Yes	No

Table 2 - 1. Admin and User Privileges

System Log Configuration

This section contains information for configuring various attributes and properties for System Log Configurations, including System Log Settings and System Log Host.

System Log Settings

This window allows the user to enable or disable the System Log and specify the System Log Save Mode Settings.

To configure the system log settings, click **Configuration > System Log Configuration > System Log Settings**

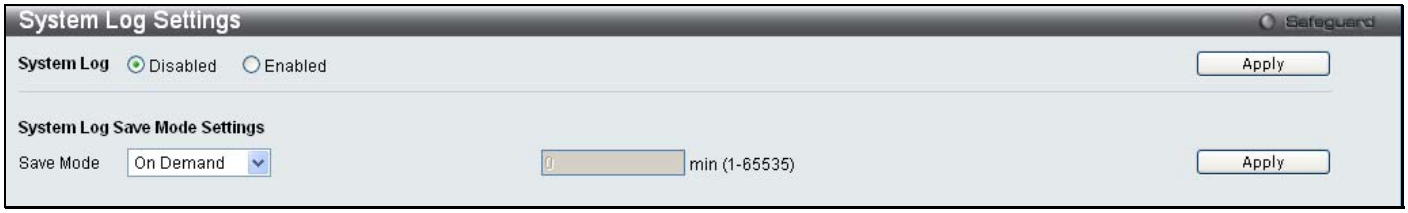


Figure 2 - 13. System Log Settings window

The following parameters can be set:

Parameter	Description
System Log	Use the radio buttons to either enable or disable the system log feature.
Save Mode	Use this drop-down menu to choose the method that will trigger a log entry. Choose among *On Demand*, *Time Interval*, and *Log Trigger*.
min (1-65535)	Enter a time interval, in minutes, for which a log entry is to be made.

To modify the system log settings on this window, enter the appropriate information and click **Apply**.

System Log Server

The Switch can send Syslog messages to up to four designated servers using the System Log Server.

To configure the system log settings, click **Configuration > System Log Configuration > System Log Server**:

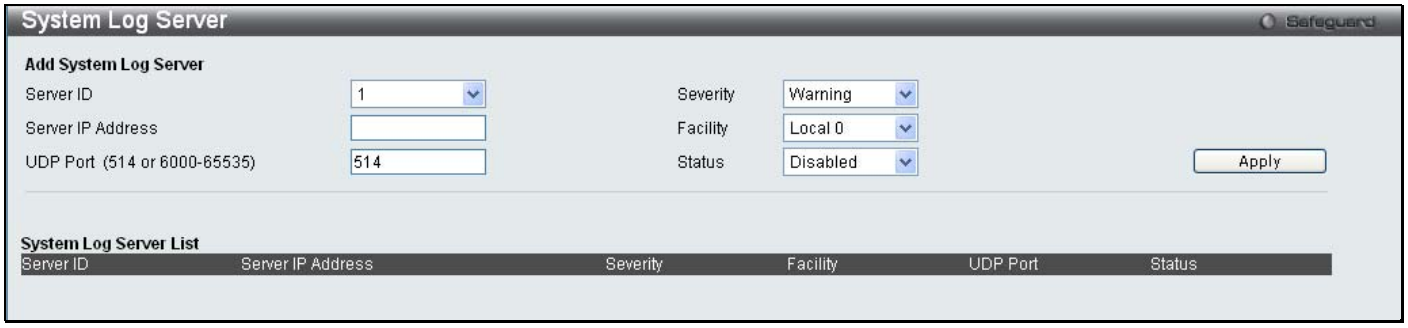


Figure 2 - 14. System Log Server window

The following parameters can be set:

Parameter	Description
Server ID	Syslog server settings index (1-4).
Severity	This drop-down menu allows you to select the level of messages that will be sent. The options are *Warning*, *Informational*, and *All*.
Server IP Address	The IP address of the Syslog server.
Facility	Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: **Bold** font indicates the facility values that the Switch is currently employing.

Numerical	Facility Code	Numerical	Facility Code
0	kernel messages	12	NTP subsystem
1	user-level messages	13	log audit
2	mail system	14	log alert
3	system daemons	15	clock daemon
4	security/authorization messages	**16**	**local use 0 (local0)**
5	messages generated internally by syslog line printer subsystem	**17**	**local use 1 (local1)**
		18	**local use 2 (local2)**
7	network news subsystem	**19**	**local use 3 (local3)**
8	UUCP subsystem	**20**	**local use 4 (local4)**
9	clock daemon	**21**	**local use 5 (local5)**
10	security/authorization messages	**22**	**local use 6 (local6)**
11	FTP daemon	**23**	**local use 7 (local7)**

UDP Port (514 or 6000-65535)	Type the UDP port number used for sending Syslog messages. The default is *514*.
Status	Choose *Enabled* or *Disabled* to activate or deactivate.

To add a new entry, enter the appropriate information and click **Apply**.

DHCP Relay

The relay hops count limit allows the maximum number of hops (routers) that the DHCP messages can be relayed through to be set. If a packet's hop count is equal to or more than the hop count limit, the packet is dropped. The range is between *1* and *16* hops, with a default value of *4*. The relay time threshold sets the minimum time (in seconds) that the Switch will wait before forwarding a BOOTREQUEST packet. If the value in the seconds field of the packet is less than the relay time threshold, the packet will be dropped. The range is between *0* and *65,535* seconds, with a default value of *0* seconds.

DHCP Relay Global Settings

To enable and configure DHCP Relay Global Settings on the Switch, click **Configuration > DHCP Relay > DHCP Relay Global Settings**:

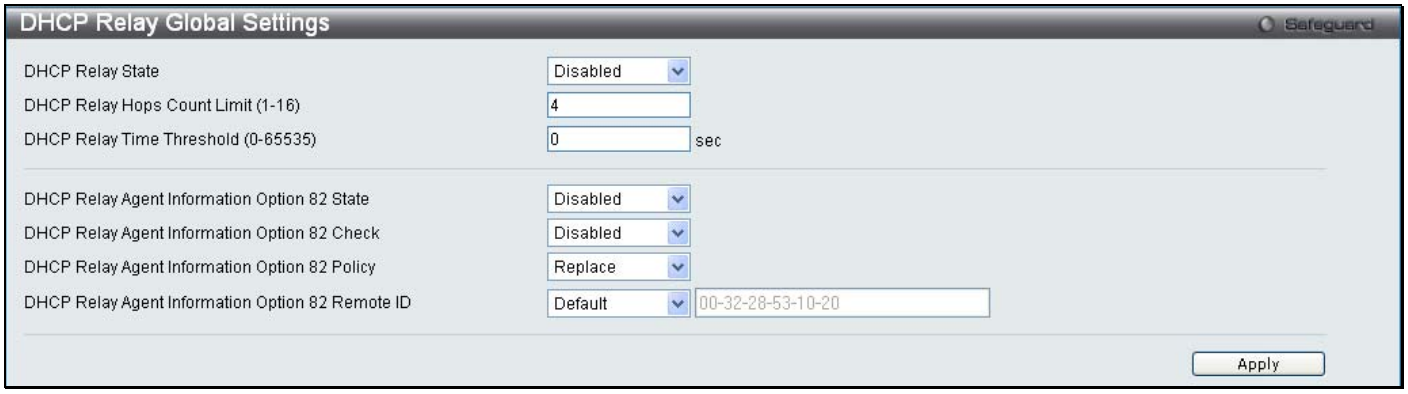


Figure 2 - 15. DHCP Relay Global Settings window

The following fields can be set:

Parameter	Description
DHCP Relay State	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. It is used to enable or disable the DHCP Relay service on the Switch. The default is *Disabled*
DHCP Relay Hops Count Limit (1-16)	This field allows an entry between *1* and *16* to define the maximum number of router hops DHCP messages can be forwarded across. The default hop count is *4*.
DHCP Relay Time Threshold (0-65535)	Allows an entry between *0* and *65535* seconds, and defines the maximum time limit for routing a DHCP packet. If a value of 0 is entered, the Switch will not process the value in the seconds field of the BOOTP or DHCP packet. If a non-zero value is entered, the Switch will use that value, along with the hop count to determine whether to forward a given BOOTP or DHCP packet.
DHCP Relay Agent Information Option 82 State	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. It is used to enable or disable the DHCP Agent Information Option 82 on the Switch. The default is *Disabled.* *Enabled* – When this field is toggled to *Enabled* the relay agent will insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients. When the relay agent receives the DHCP request, it adds the option 82 information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option 82 information has been added to the packet it is sent on to the DHCP server. When the DHCP server receives the packet, if the server is capable of option 82, it can implement policies like restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option 82 field in the DHCP reply. The DHCP server unicasts the reply to the back to the relay agent if the request was relayed to the server by the relay agent. The switch verifies that it originally inserted the option 82 data. Finally, the relay agent removes the option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request. *Disabled* - If the field is toggled to *Disabled* the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the

	check and policy settings will have no effect.
DHCP Relay Agent Information Option 82 Check	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. It is used to enable or disable the Switches ability to check the validity of the packet's option 82 field. *Enabled* – When the field is toggled to *Enable*, the relay agent will check the validity of the packet's option 82 field. If the switch receives a packet that contains the option-82 field from a DHCP client, the switch drops the packet because it is invalid. In packets received from DHCP servers, the relay agent will drop invalid messages. *Disabled* - When the field is toggled to *Disabled*, the relay agent will not check the validity of the packet's option 82 field.
DHCP Relay Agent Information Option 82 Policy	This field can be toggled between *Replace, Drop,* and *Keep* by using the pull-down menu. It is used to set the Switches policy for handling packets when the DHCP Agent Information Option 82 Check is set to *Disabled*. The default is *Replace.* *Replace* - The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client. *Drop* - The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client. *Keep* -The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.
DHCP Relay Agent Information Option 82 Remote ID	This field is for you to enter the remote ID. Tick Default to use the Switch's system MAC address as the remote ID.

Click **Apply** to implement any changes that have been made.

NOTE: If the Switch receives a packet that contains the option-82 field from a DHCP client and the information-checking feature is enabled, the switch drops the packet because it is invalid. However, in some instances, you might configure a client with the option-82 field. In this situation, you should disable the information-check feature so that the switch does not remove the option-82 field from the packet. You can configure the action that the switch takes when it receives a packet with existing option-82 information by configuring the DHCP Agent Information Option 82 Policy.

The Implementation of DHCP Information Option 82 on the Switch

The **config dhcp_relay option_82** command configures the DHCP relay agent information option 82 setting of the switch. The formats for the circuit ID sub-option and the remote ID sub-option are as follows:

NOTE: For the circuit ID sub-option of a standalone switch, the module field is always zero.

Circuit ID sub-option format:

a.	b.	c.	d.	e.	f.	g.
1	6	0	4	VLAN	Module	Port
1 byte	1 byte	1 byte	1 byte	2 bytes	1 byte	1 byte

a. Sub-option type
b. Length
c. Circuit ID type
d. Length
e. VLAN: the incoming VLAN ID of DHCP client packet.
f. Module: For a standalone switch, the Module is always 0; For a stackable switch, the Module is the Unit ID.
g. Port: The incoming port number of DHCP client packet, port number starts from 1.

Remote ID sub-option format: (default)

1.	2.	3.	4.	5.
2	8	0	6	MAC address
1 byte	1 byte	1 byte	1 byte	6 bytes

1. Sub-option type
2. Length
3. Remote ID type
4. Length
5. MAC address: The Switch's system MAC address.

Remote ID sub-option format:(for user-configured string)

1.	2.	3.	4.	5.
2	N+2	1	N	ASCII Remote ID String (up to 127 characters)
1 byte	1 byte	1 byte	1 byte	N bytes

1. Sub-option type
2. Length
3. Remote ID type
4. Length
5. User configured Remote-ID

Figure 2 - 16. Circuit ID and Remote ID Sub-option Format

DHCP Relay Interface Settings

This window allows the user to set up a server, by IP address, for relaying DHCP/ BOOTP information to the Switch. The user may enter a previously configured IP interface on the Switch that will be connected directly to the DHCP server using the following window. Properly configured settings will be displayed in the DHCP Relay Interface Table at the bottom of the following window. The user may add up to four server IP's per IP interface on the Switch.

To enable and configure DHCP Relay Global Settings on the Switch, click **Configuration > DHCP Relay > DHCP Relay Interface Settings**:

Figure 2 - 17. DHCP Relay Interface Settings window

The following parameters may be configured or viewed.

Parameter	Description
Interface	The IP interface on the Switch that will be connected directly to the Server.
Server IP	Enter the IP address of the DHCP server. Up to four server IPs can be configured per IP Interface

DHCP Local Relay Settings

This function on the Switch allows configuration of the DHCP local relay for VLAN.

To view this window, click **Configuration > DHCP Local Relay> DHCP Local Relay Settings**:

Figure 2 - 18. DHCP Local Relay Settings window

The following parameters may be configured.

Parameter	Description
DHCP Local Relay Operation State	This is used to enable or disable DHCP Local Relay service on the Switch. The default is Disabled.
VLAN Name	Enter a name of the VLAN to be enabled by DHCP local relay.
VID List	Enter a VLAN ID to be enabled by DHCP local relay.

State	This is used to enable or disable the DHCP local relay for the specified VLAN.

DHCP Auto Configuration Settings

The DHCP automatic configuration function on the Switch will load a previously saved configuration file for current use. When DHCP auto configuration is Enabled on the Switch, the DHCP reply will contain a configuration file and path name. It will then request the file from the TFTP server specified in the reply.

To view this window, click **Configuration > DHCP Auto Configuration Settings**:

Figure 2 - 19. DHCP Auto Configuration Settings window

When DHCP automatic configuration is Enabled, the Switch becomes a DHCP client automatically after rebooting. The DHCP server must have the TFTP server IP address and configuration file name, and be configured to deliver this information in the data field of the DHCP reply packet. The TFTP server must be running and have the requested configuration file in its base directory when the request is received from the Switch. Consult the DHCP server and TFTP server software instructions for information on loading a configuration file.

If the Switch is unable to complete the automatic configuration process, the previously saved local configuration file present in Switch memory will be loaded.

MAC Address Aging Time

This table specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). To change this, enter a value representing the MAC address age-out time in seconds. The MAC Address Aging Time can be set to any value between *10* and *1,000,000* seconds. The default setting is *300* seconds.

To access this window, click **Configuration > MAC Address Aging Time**:

Figure 2 - 20. MAC Address Aging Time window

Web Settings

Web-based management is Enabled by default. If you choose to disable this by selecting Disabled, you will lose the ability to configure the system through the Web interface as soon as these settings are applied. The TCP ports are numbered between *1* and *65535*. The "well-known" TCP port for the Web protocol is *80*.

To access this window, click **Configuration > Web Settings**:

Figure 2 - 21. Web Settings window

Telnet Settings

Telnet configuration is Enabled by default. If you do not want to allow configuration of the system through Telnet choose Disabled. The TCP ports are numbered between *1* and *65535*. The "well-known" TCP port for the Telnet protocol is *23*.

To access this window, click **Configuration > Telnet Settings**:

Figure 2 - 22. Telnet Settings window

Password Encryption

Password Encryption can be Enabled or Disabled in this window. It is Disabled by default. Password encryption allows the user to encrypt a password for additional security. Select Enabled to change the password into encrypted form. When password encryption is Disabled, the password will be in plain text form. However, if the user specifies the password in encrypted form, or if the password has been converted to encrypted form by the last **enable password encryption** command, the password will still be in encrypted form and cannot be reverted back to plain text form.

To access this window, click **Configuration > Password Encryption**:

Figure 2 - 23. Password Encryption window

CLI Paging Settings

CLI paging can be Enabled or Disabled in this window. It is Enabled by default. CLI paging settings are used when issuing a command which causes the console screen to rapidly scroll through several pages. This command will cause the console to pause at the end of each page.

To access this window, click **Configuration > CLI Paging Settings**:

Figure 2 - 24. CLI Paging Settings window

Firmware Information

Information about current firmware images stored on the Switch can be viewed.

To access this window, click **Configuration > Firmware Information**:

Figure 2 - 25. Firmware Information window

This window holds the following information:

Parameter	Description
ID	States the image ID number of the firmware in the Switch's memory. The Switch can store two firmware images for use. Image ID 1 will be the default boot up firmware for the Switch unless otherwise configured by the user.
Version	States the firmware version.
Size (Bytes)	States the size of the corresponding firmware, in bytes.
Update Time	States the specific time the firmware version was downloaded to the Switch.
From	States the IP address of the origin of the firmware.
User	States the user who downloaded the firmware. This field may read "Anonymous" or "Unknown" for users that are unidentified.

SNTP Settings

The SNTP Settings folder offers two windows: **Time Settings** and **Time Zone Settings**.

Time Settings

To configure the time settings for the Switch, click **Configuration > SNTP Settings > Time Settings**:

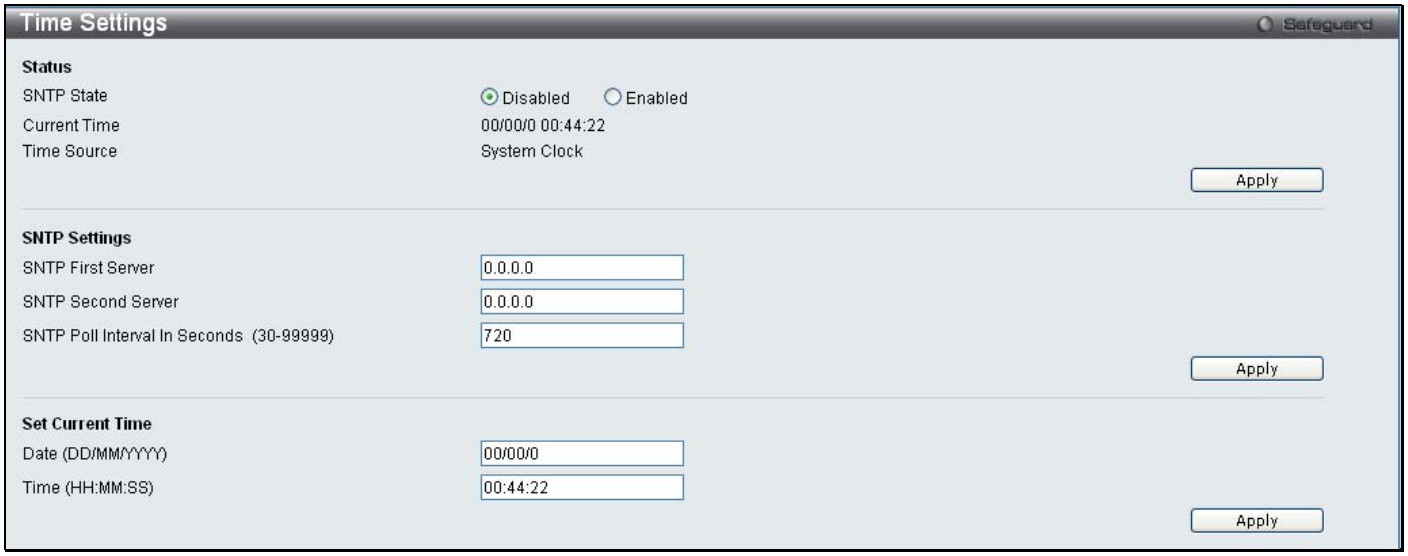


Figure 2 - 26. Time Settings window

The following parameters can be set or are displayed:

Parameter	Description
Status	
SNTP State	Use the radio button to select an Enabled or Disabled SNTP state.
Current Time	Displays the Current Time set on the Switch.
Time Source	Displays the time source for the system.
SNTP Settings	
SNTP First Server	This is the IP address of the primary server the SNTP information will be taken from.
SNTP Second Server	This is the IP address of the secondary server the SNTP information will be taken from.
SNTP Poll Interval in Seconds (30-99999)	This is the interval, in seconds, between requests for updated SNTP information.
Set Current Time	
Date (DD/MM/YYYY)	Enter the current date in day, month and year to update the system clock.
Time (HH:MM:SS)	Enter the current time in hours, minutes, and seconds.

Click **Apply** to implement changes made.

Time Zone Settings

The following window is used to configure time zones and Daylight Savings Time settings for SNTP.

To configure the time zone settings for the Switch, click **Configuration > SNTP Settings > Time Zone Settings**:

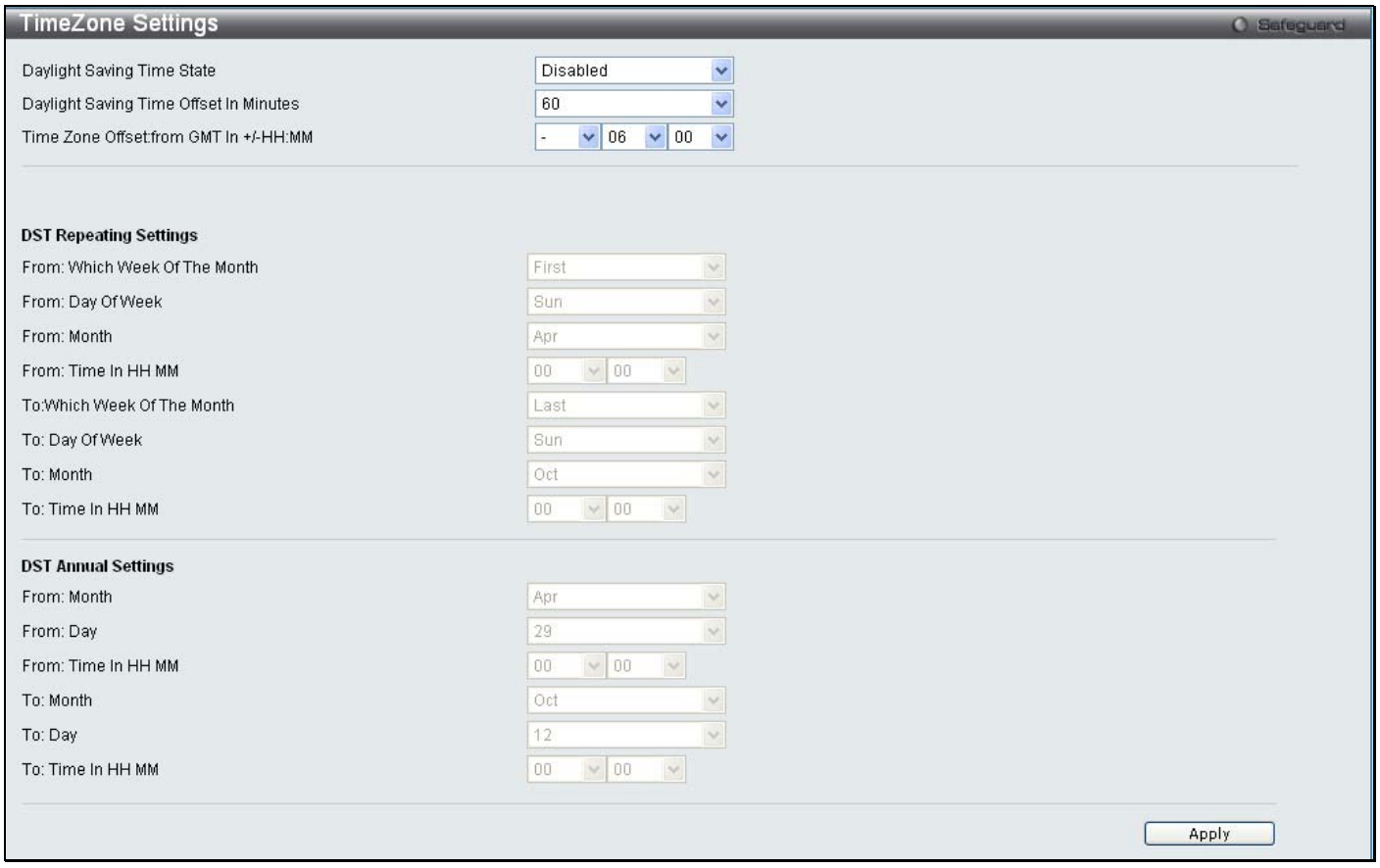


Figure 2 - 27. Time Zone Settings window

The following parameters can be set:

Parameter	Description
Time Zone and DST	
Daylight Saving Time State	Use this pull-down menu to enable or disable the DST Settings.
Daylight Saving Time Offset in Minutes	Use this pull-down menu to specify the amount of time that will constitute your local DST offset *30*, *60*, *90*, or *120* minutes.
Time Zone Offset from GMT in +/- HH:MM	Use these pull-down menus to specify your local time zone's offset from Greenwich Mean Time (GMT.)
DST Repeating Settings Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October.	
From: Which Week of the Month	Enter the week of the month that DST will start on.

From: Day of the Week	Enter the day of the week that DST will start on.
From: Month	Enter the month DST will start on.
From: Time in HH:MM	Enter the time of day that DST will start on.
To: Which Week of the Month	Enter the week of the month the DST will end.
To: Day of the Week	Enter the day of the week that DST will end.
To: Month	Enter the month that DST will end.
To:Time in HH:MM	Enter the time DST will end.
DST Annual Settings Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14.	
From: Month	Enter the month DST will start on, each year.
From: Day	Enter the day of the week DST will start on, each year.
From: Time in HH:MM	Enter the time of day DST will start on, each year.
To: Month	Enter the month DST will end, each year.
To: Day	Enter the date DST will end, each year.
To: Time in HH:MM	Enter the time of day that DST will end, each year.

Click **Apply** to implement changes made in this window.

SMTP Settings

SMTP or Simple Mail Transfer Protocol is a function of the Switch that will send switch events to mail recipients based on e-mail addresses entered in the window below. The Switch is to be configured as a client of SMTP while the server is a remote device that will receive messages from the Switch, place the appropriate information into an e-mail and deliver it to recipients configured on the Switch. This can benefit the Switch administrator by simplifying the management of small workgroups or wiring closets, increasing the speed of handling emergency Switch events, and enhancing security by recording questionable events occurring on the Switch.

Users can set up the SMTP server for the Switch, along with setting e-mail addresses to which switch log files can be sent when a problem arises on the Switch.

SMTP Service Settings

To view the following window, click **Configuration > SMTP Service Settings**:

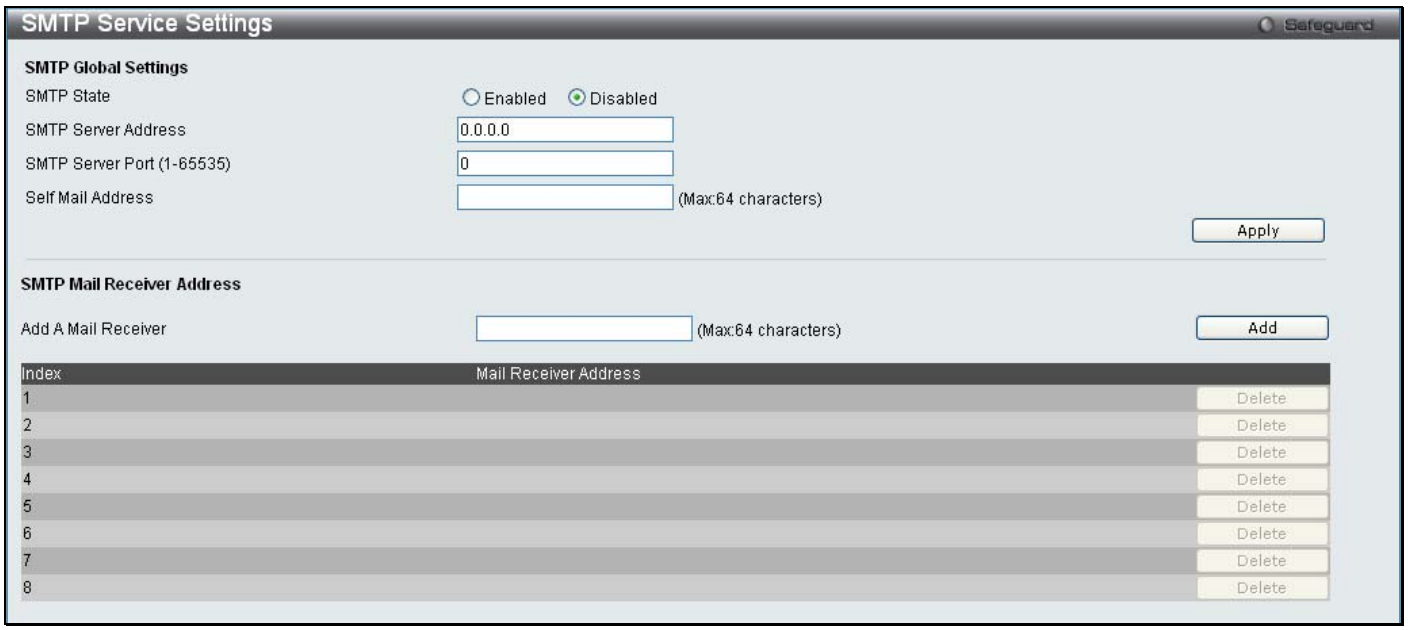


Figure 2 - 28. SMTP Service Settings window

The following parameters may be configured or viewed:

Parameter	Description
SMTP State	Use the radio button to enable or disable the SMTP service on this device.
SMTP Server Address	Enter the IP address of the SMTP server on a remote device. This will be the device that sends out the mail for you.
SMTP Server Port (1-65535)	Enter the virtual port number that the Switch will connect with on the SMTP server. The common port number for SMTP is *25*, yet a value between *1* and *65535* can be chosen.
Self Mail Address	Enter the e-mail address from which mail messages will be sent. This address will be the "from" address on the e-mail message sent to a recipient. Only one self-mail address can be configured for this Switch. This string can be no more that 64 alphanumeric characters.
Add A Mail Receiver	Enter an e-mail address and click the **Add** button. Up to eight e-mail addresses can be added per Switch. To delete these addresses from the Switch, click the corresponding **Delete** button in the SMTP Mail Receiver Address table at the bottom of the window.

SMTP Service

This window is used to test the SMTP Service Settings configured in the previous window.

To view the following window, click **Configuration > SMTP Service**:

Figure 2 - 29. SMTP Service window

To test to see if the SMTP settings are working properly, enter a Subject, Content, and then click the **Send** button.

MAC Notification Settings

MAC Notification is used to monitor MAC addresses learned and entered into the forwarding database. To globally set MAC notification on the Switch, open the following window by opening the **MAC Notification Settings** in the Configuration folder.

MAC Notification Global Settings

To configure the MAC Notification Global Settings for the Switch, click **Configuration > MAC Notification Settings > MAC Notification Global Settings**

Figure 2 - 30. MAC Notification Global Settings window

The following parameters may be viewed and modified:

Parameter	Description
State	Enable or disable MAC notification globally on the Switch.
Interval (1-2147483647 sec)	The time in seconds between notifications.
History Size (1-500)	The maximum number of entries listed in the history log used for notification. Up to 500 entries can be specified.

Click **Apply** to implement changes.

MAC Notification Port Settings

To configure the MAC Notification Port Settings for the Switch, click **Configuration > MAC Notification Settings > MAC Notification Port Settings**:

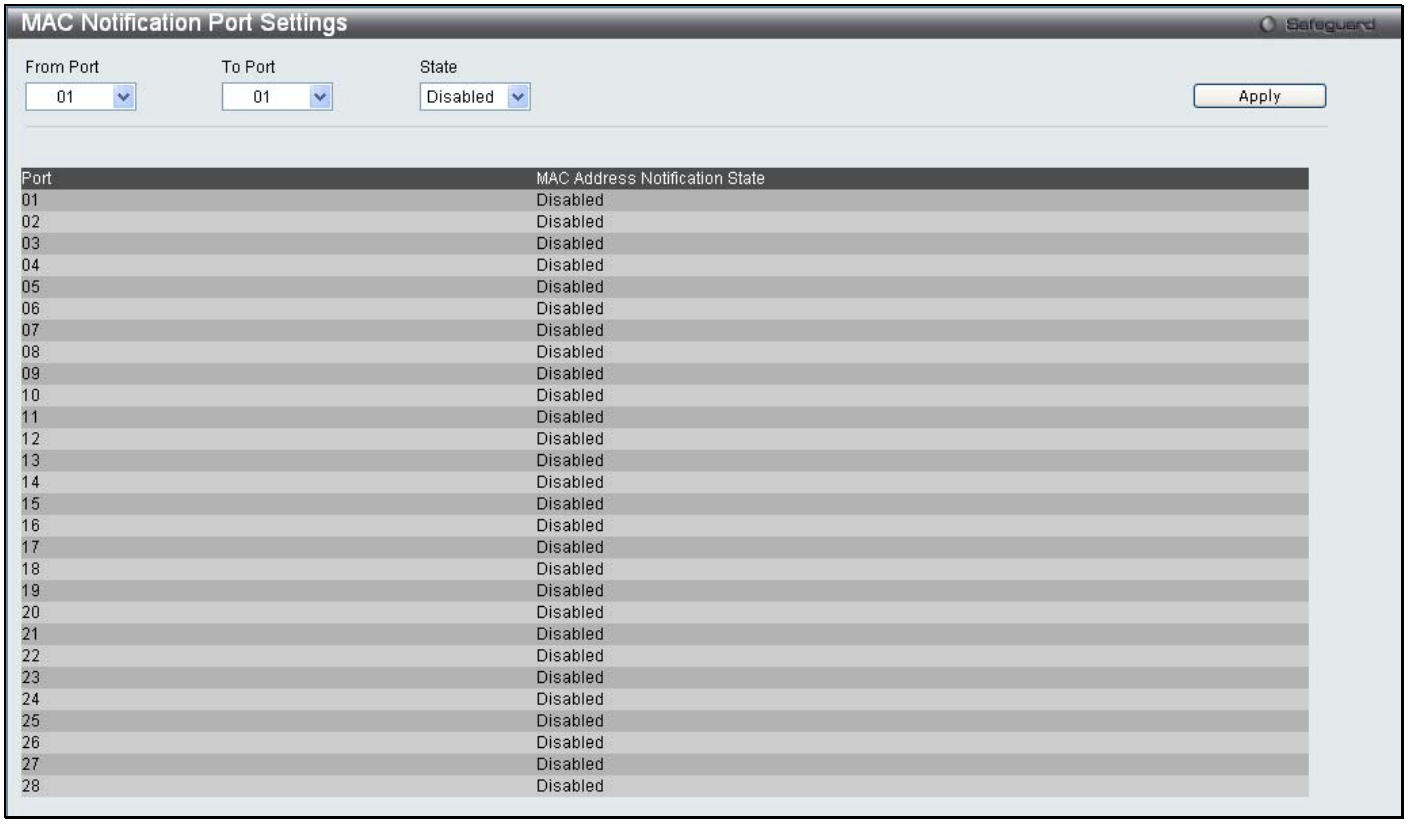


Figure 2 - 31. MAC Notification Port Settings window

The following parameters may be modified:

Parameter	Description
From Port/To Port	Select a port or group of ports to enable for MAC notification using the pull-down menus.
State	Enable MAC Notification for the ports selected using the pull-down menu.

Click **Apply** to implement changes.

SNMP Settings

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch, switch group or network.

Managed devices that support SNMP include software (referred to as an agent), which runs locally on the device. A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The Switch supports the SNMP versions 1, 2c, and 3. Choose which version to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

In SNMP v.1 and v.2, user authentication is accomplished using 'community strings', which function like passwords. The remote user SNMP application and the Switch SNMP must use the same community string. SNMP packets from any station that has not been authenticated are ignored (dropped).

The default community strings for the Switch used for SNMP v.1 and v.2 management access are:

- **public** - Allows authorized management stations to retrieve MIB objects.
- **private** - Allows authorized management stations to retrieve and modify MIB objects.

SNMPv3 uses a more sophisticated authentication process that is separated into two parts. The first part is to maintain a list of users and their attributes that are allowed to act as SNMP managers. The second part describes what each user on that list can do as an SNMP manager.

The Switch allows groups of users to be listed and configured with a shared set of privileges. The SNMP version may also be set for a listed group of SNMP managers. Thus, you may create a group of SNMP managers that are allowed to view read-only information or receive traps using SNMPv1 while assigning a higher level of security to another group, granting read/write privileges using SNMPv3.

Using SNMPv3 individual users or groups of SNMP managers can be allowed to perform or be restricted from performing specific SNMP management functions. The functions allowed or restricted are defined using the Object Identifier (OID) associated with a specific MIB. An additional layer of security is available for SNMPv3 in that SNMP messages may be encrypted. To read more about how to configure SNMPv3 settings for the Switch read the next section.

Traps

Traps are messages that alert network personnel of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned OFF the Switch), or less serious like a port status change. The Switch generates traps and sends them to the trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, Topology Change and Broadcast\Multicast Storm.

MIBs

The Switch in the Management Information Base (MIB) stores management and counter information. The Switch uses the standard MIB-II Management Information Base module. Consequently, values for MIB objects can be retrieved from any SNMP-based network management software. In addition to the standard MIB-II, the Switch also supports its own proprietary enterprise MIB as an extended Management Information Base. Specifying the MIB Object Identifier may also retrieve the proprietary MIB. MIB values can be either read-only or read-write.

The Switch incorporates a flexible SNMP management for the switching environment. SNMP management can be customized to suit the needs of the networks and the preferences of the network administrator.

The Switch supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. The administrator can specify the SNMP version used to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

SNMP View Table

This window is used to assign views to community strings or SNMP groups that define which MIB objects can be accessed by a remote SNMP manager.

To configure SNMP View Settings for the Switch, click **Configuration > SNMP Settings > SNMP View Table**:

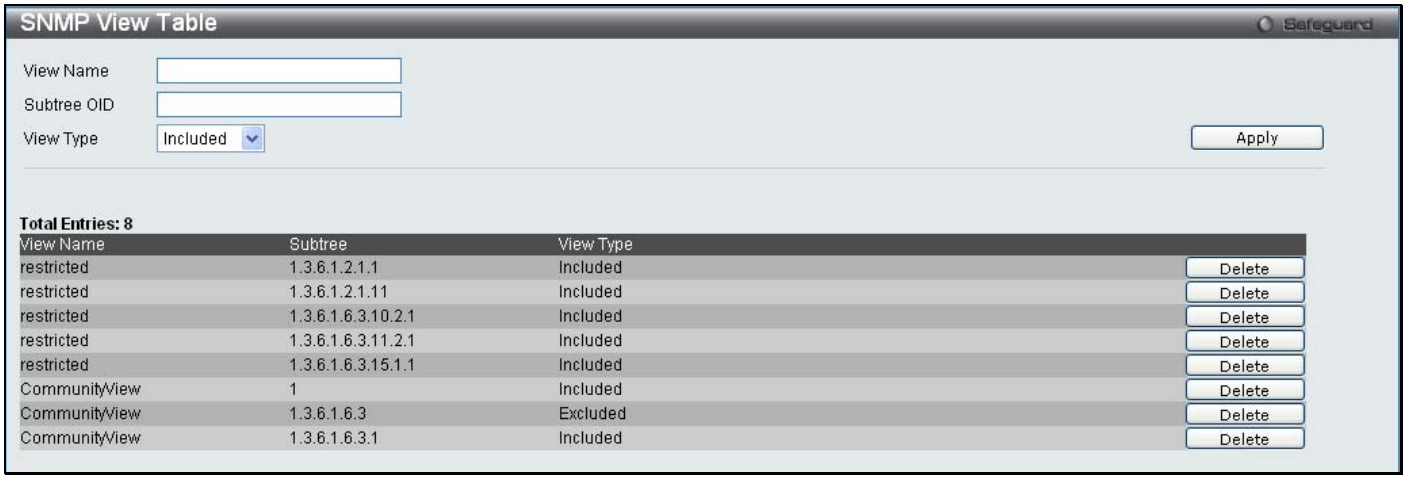


Figure 2 - 32. SNMP View Table window

The following parameters can be set:

Parameter	Description
View Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP view being created.
Subtree OID	Type the Object Identifier (OID) Subtree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.
View Type	Select *Included* to include this object in the list of objects that an SNMP manager can access. Select *Excluded* to exclude this object from the list of objects that an SNMP manager can access.

To implement your new settings, click **Apply**. To delete an entry click the corresponding **Delete** button.

SNMP Group Table

An SNMP Group created with this table maps SNMP users (identified in the **SNMP User Table** window) or community strings to the views created in the previous window.

To view this window, click **Configuration > SNMP Settings > SNMP Group Table**:

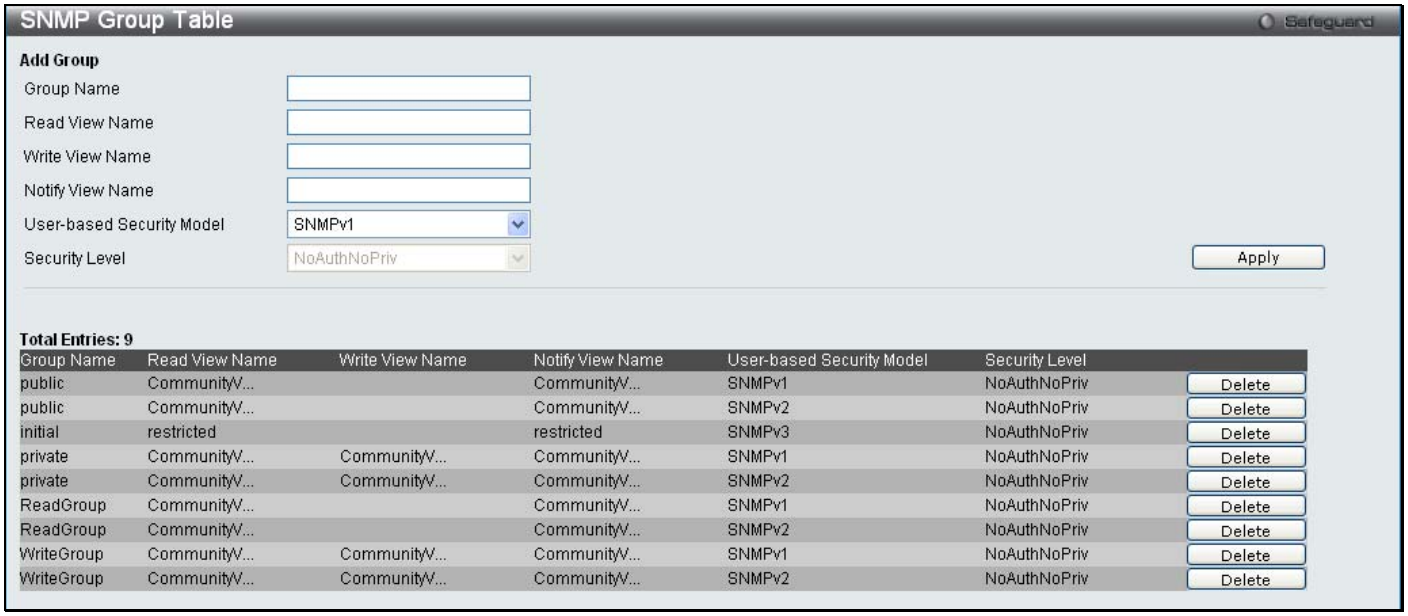


Figure 2 - 33. SNMP Group Table window

To delete an existing SNMP Group Table entry, click the corresponding **Delete** button.

The following parameters can be set:

Parameter	Description
Group Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP group of SNMP users.
Read View Name	Specify an SNMP group name for users that are allowed SNMP read privileges to the Switch's SNMP agent.
Write View Name	Specify an SNMP group name for users that are allowed SNMP write privileges to the Switch's SNMP agent.
Notify View Name	Specify an SNMP group name for users that can receive SNMP trap messages generated by the Switch's SNMP agent.
User-based Security Model	*SNMPv1* - Specifies that SNMP version 1 will be used. *SNMPv2* - Specifies that SNMP version 2c will be used. The SNMPv2 supports both

	centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *SNMPv3* - Specifies that the SNMP version 3 will be used. SNMPv3 provides secure access to devices through a combination of authentication and encrypting packets over the network.
Security Level	The Security Level settings only apply to SNMPv3. *NoAuthNoPriv* - Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *AuthNoPriv* - Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. *AuthPriv* - Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.

To implement the new settings, click **Apply**.

SNMP User Table

This window displays all of the SNMP User's currently configured on the Switch and also allows you to add new users.

To view this window, click **Configuration > SNMP Settings > SNMP User Table**:

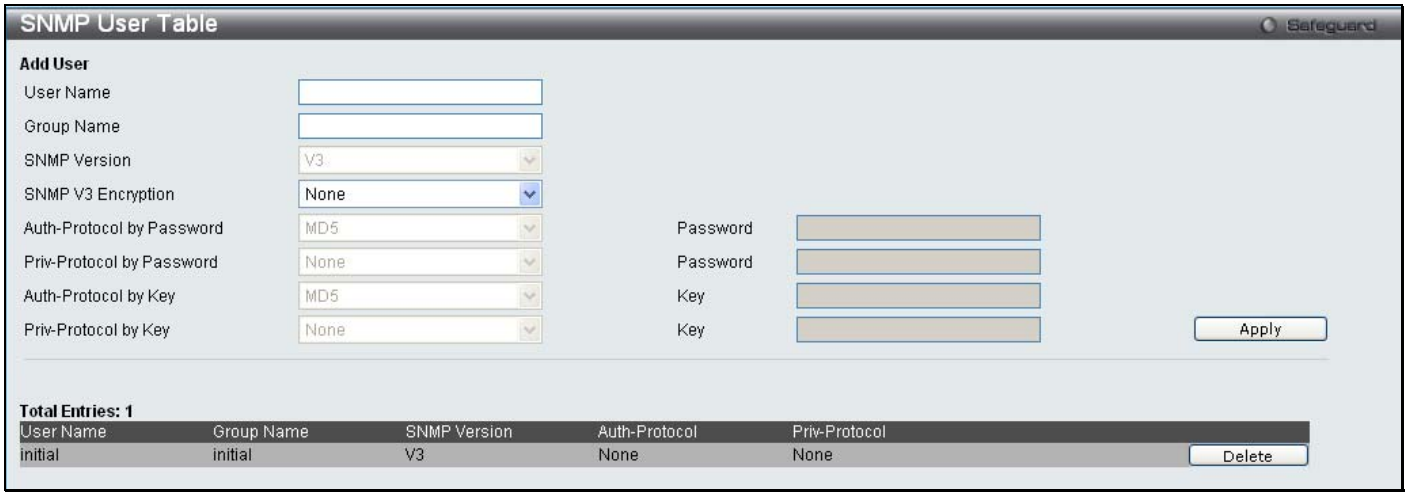


Figure 2 - 34. SNMP User Table window

To delete an existing **SNMP User Table** entry, click the corresponding **Delete** button.

The following parameters may be set:

Parameter	Description
User Name	An alphanumeric string of up to 32 characters. This is used to identify the SNMP users.
Group Name	This name is used to specify the SNMP group created can request SNMP messages.
SNMP Version	*V1* - Indicates that SNMP version 1 is in use. *V2* - Indicates that SNMP version 2 is in use. *V3* - Indicates that SNMP version 3 is in use.
SNMP V3 Encryption	*None* – Indicates that there is no SNMP V3 Encryption *Password* – Indicates that there is SNMP V3 Encryption through a password *Key* – Indicates that there is SNMP V3 Encryption through a key.
Auth-Protocol by Password	*MD5* - Indicates that the HMAC-MD5-96 authentication level will be used. *SHA* - Indicates that the HMAC-SHA authentication protocol will be used.

Priv-Protocol by Password	*None* - Indicates that no authorization protocol is in use. *DES* - Indicates that DES 56-bit encryption is in use based on the CBC-DES (DES-56) standard.
Auth-Protocol by Key	*MD5* - Indicates that the HMAC-MD5-96 authentication level will be used. *SHA* - Indicates that the HMAC-SHA authentication protocol will be used.
Priv-Protocol by Key	*None* - Indicates that no authorization protocol is in use. *DES* - Indicates that DES 56-bit encryption is in use based on the CBC-DES (DES-56) standard.
Password	Enter a Password when SNMP V3 Encryption is enabled for Password mode.
Key	Enter a Key when SNMP V3 Encryption is enabled for Key mode.

To implement changes made, click **Apply**.

SNMP Community Table

Use this table to view existing SNMP Community Table configurations and to create a SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string:

Any MIB view that defines the subset of all MIB objects will be accessible to the SNMP community.

Read/write or read-only level permission for the MIB objects accessible to the SNMP community.

To configure SNMP Community entries, click **Configuration > SNMP Settings > SNMP Community Table**:

Figure 2 - 35. SNMP Community Table window

The following parameters can set:

Parameter	Description
Community Name	Type an alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.
View Name	Type an alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. The view name must exist in the SNMP View Table.
Access Right	*Read Only* - Specifies that SNMP community members using the community string created can only read the contents of the MIBs on the Switch. *Read Write* - Specifies that SNMP community members using the community string created can read from, and write to the contents of the MIBs on the Switch.

To implement the new settings, click **Apply**. To delete an entry from the **SNMP Community Table**, click the corresponding **Delete** button.

SNMP Host Table

Use the **SNMP Host Table** window to set up SNMP trap recipients. To configure SNMP Host Table entries, click **Configuration > SNMP Settings > SNMP Host Table**

Figure 2 - 36. SNMP Host Table window

The following parameters can set:

Parameter	Description
Host IP Address	Type the IP address of the remote management station that will serve as the SNMP host for the Switch.
User-based Security Model	*SNMPv1* - Specifies that SNMP version 1 will be used. *SNMPV2c* - Specifies that SNMP version 2 will be used. *SNMPV3* - To specify that the SNMP version 3 will be used.
Security Level	*NoAuthNoPriv* – To specify a NoAuthNoPriv security level. *AuthNoPriv* - To specify an AuthNoPriv security level. *AuthPriv* - To specify an AuthPriv security level.
Community String/ SNMPv3 User Name	Type in the community string or SNMPv3 user name as appropriate.

To implement your new settings, click **Apply**.

SNMP Engine ID

The Engine ID is a unique identifier used for SNMP V3 implementations. This is an alphanumeric string used to identify the SNMP engine on the Switch.

To display the Switch's SNMP Engine ID, click **Configuration > SNMP Settings > SNMP Engine ID**:

Figure 2 - 37. SNMP Engine ID window

To change the Engine ID, enter the new Engine ID in the space provided and click the **Apply** button.

SNMP Trap Configuration

The following window is used to enable and disable trap settings for the SNMP function on the Switch.

To view this window for configuration, click **Configuration > SNMP Settings > SNMP Trap Configuration**:

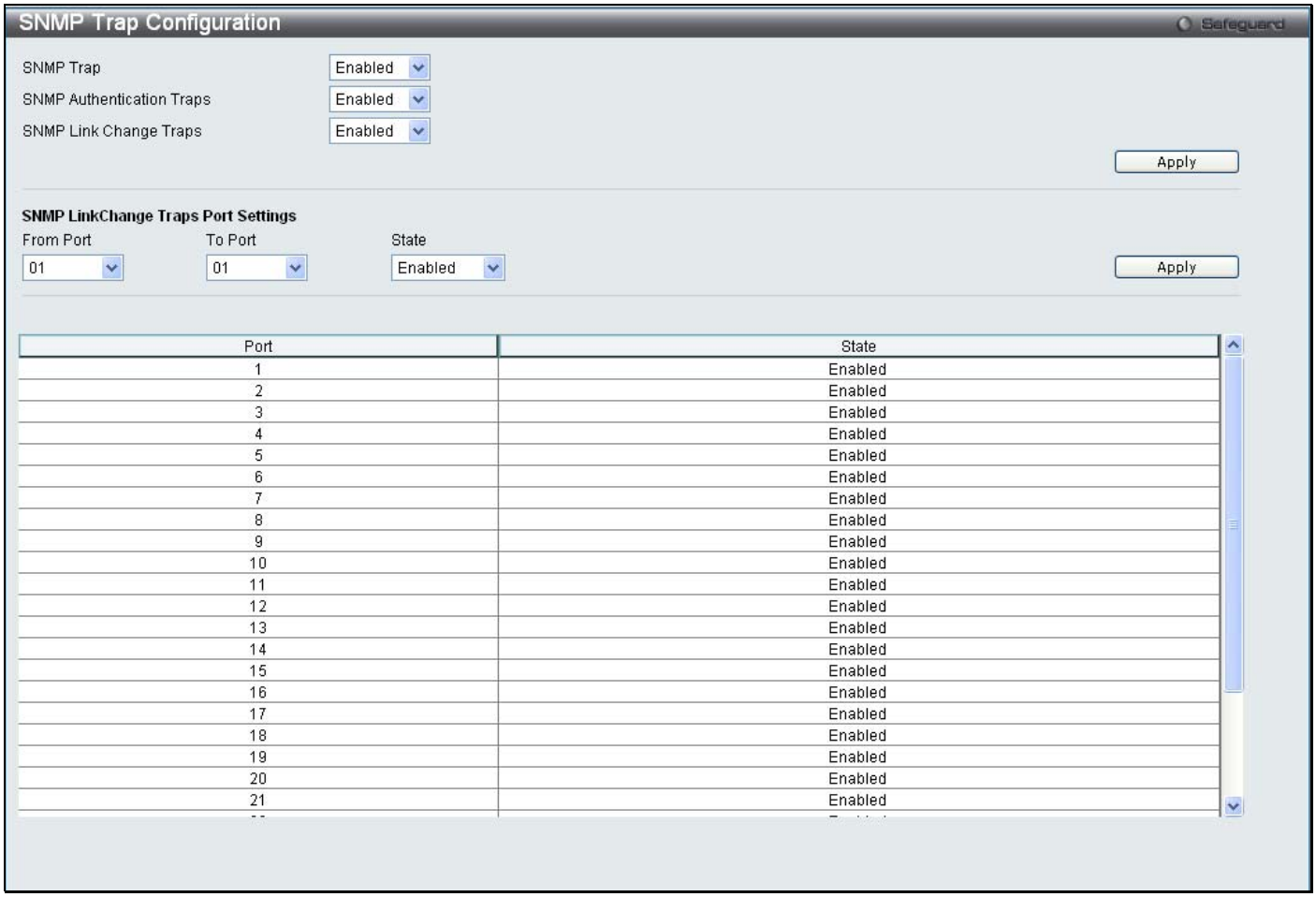


Figure 2 - 38. SNMP Trap Configuration window

To enable or disable the SNMP Trap State, SNMP Authentication Traps, SNMP Link Change Traps, and configure SNMP Link Change Trap Port Settings, use the corresponding pull-down menus. Click **Apply** to let the changes take effect.

RMON

Users can enable and disable remote monitoring (RMON) status for the SNMP function on the Switch.

To view this window for configuration, click **Configuration > SNMP Settings > RMON**:

Figure 2 - 39. RMON window

To enable or disable RMON for SNMP, use the radio button. Click **Apply** when finished.

Time Range Settings

This window is used in conjunction with the Access Profile feature to determine a starting point and an ending point, based on days of the week, when an Access Profile configuration will be enabled on the Switch. Once configured here, the time range settings are to be applied to an access profile rule using the Access Profile table. The user may enter up to 64 time range entries on the Switch.

To open this window, click **Configuration > Time Range Settings**:

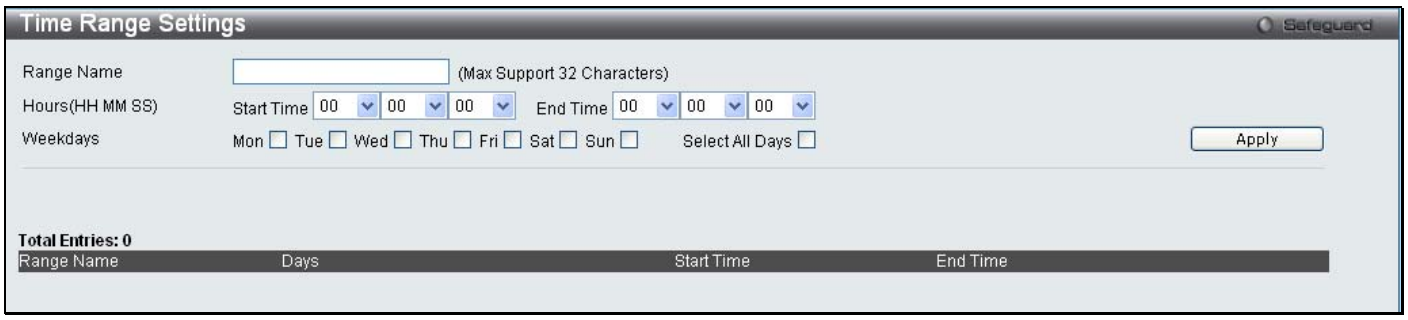


Figure 2 - 40. Time Range Settings window

Single IP Management

Simply put, D-Link Single IP Management is a concept that will stack switches together over Ethernet instead of using stacking ports or modules. There are some advantages in implementing the "Single IP Management" feature:

1. SIM can simplify management of small workgroups or wiring closets while scaling the network to handle increased bandwidth demand.
2. SIM can reduce the number of IP address needed in your network.
3. SIM can eliminate any specialized cables for stacking connectivity and remove the distance barriers that typically limit your topology options when using other stacking technology.

Switches using D-Link Single IP Management (labeled here as SIM) must conform to the following rules:

SIM is an optional feature on the Switch and can easily be enabled or disabled through the Command Line Interface or Web Interface. SIM grouping has no effect on the normal operation of the Switch in the user's network.

There are three classifications for SIM. The Commander Switch (CS), which is the master switch of the group, Member Switch (MS), which is a switch that is recognized by the CS a member of a SIM group, and a Candidate Switch (CaS), which is a Switch that has a physical link to the SIM group but has not been recognized by the CS as a member of the SIM group.

A SIM group can only have one Commander Switch (CS).

All switches in a particular SIM group must be in the same IP subnet (broadcast domain). Members of a SIM group cannot cross a router.

A SIM group accepts up to 33 switches (numbered 0-32), including the Commander Switch (numbered 0).

There is no limit to the number of SIM groups in the same IP subnet (broadcast domain), however a single switch can only belong to one group.

If multiple VLANs are configured, the SIM group will only utilize the system VLAN on any switch.

SIM allows intermediate devices that do not support SIM. This enables the user to manage switches that are more than one hop away from the CS.

The SIM group is a group of switches that are managed as a single entity. SIM switches may take on three different roles:

1. **Commander Switch (CS)** - This is a switch that has been manually configured as the controlling device for a group, and takes on the following characteristics:

   It has an IP Address.

   It is not a commander switch or member switch of another Single IP group.

   It is connected to the member switches through its management VLAN.
2. **Member Switch (MS)** - This is a switch that has joined a single IP group and is accessible from the CS, and it takes on the following characteristics:

   It is not a CS or MS of another Single IP group.

It is connected to the CS through the CS management VLAN.

3. **Candidate Switch (CaS)** - This is a switch that is ready to join a SIM group but is not yet a member of the SIM group. The Candidate Switch may join the SIM group of a switch by manually configuring it to be a MS of a SIM group. A switch configured as a CaS is not a member of a SIM group and will take on the following characteristics:

It is not a CS or MS of another Single IP group.

It is connected to the CS through the CS management VLAN

After configuring one switch to operate as the CS of a SIM group, additional switches may join the group through a direct connection to the Commander switch. Only the Commander switch will allow entry to the candidate switch enabled for SIM. The CS will then serve as the in band entry point for access to the MS. The CS's IP address will become the path to all MS's of the group and the CS's Administrator's password, and/or authentication will control access to all MS's of the SIM group.

With SIM enabled, the applications in the CS will redirect the packet instead of executing the packets. The applications will decode the packet from the administrator, modify some data, then send it to the MS. After execution, the CS may receive a response packet from the MS, which it will encode and send it back to the administrator.

When a CaS becomes a MS, it automatically becomes a member of the first SNMP community (include read/write and read only) to which the CS belongs. However, if a MS has its own IP address, it can belong to SNMP communities to which other switches in the group, including the CS, do not belong.

The Upgrade to v1.6

To better improve SIM management, the Switch has been upgraded to version 1.6 in this release. Many improvements have been made, including:

1. The Commander Switch (CS) now has the capability to automatically rediscover member switches that have left the SIM group, either through a reboot or web malfunction. This feature is accomplished through the use of Discover packets and Maintain packets that previously set SIM members will emit after a reboot. Once a MS has had its MAC address and password saved to the CS's database, if a reboot occurs in the MS, the CS will keep this MS information in its database and when a MS has been rediscovered, it will add the MS back into the SIM tree automatically. No configuration will be necessary to rediscover these switches.

There are some instances where pre-saved MS switches cannot be rediscovered. For example, if the Switch is still powered down, if it has become the member of another group, or if it has been configured to be a Commander Switch, the rediscovery process cannot occur.

2. The topology map now includes new features for connections that are a member of a port trunking group. It will display the speed and number of Ethernet connections creating this port trunk group.

3. This version will support multiple switch upload and downloads for firmware, configuration files and log files, as follows:

- **Firmware** – The switch now supports multiple MS firmware downloads from a TFTP server.
- **Configuration Files** – This switch now supports multiple downloading and uploading of configuration files both to (for configuration restoration) and from (for configuration backup) MS's, using a TFTP server..
- **Log** – The switch now supports uploading multiple MS log files to a TFTP server.

4. The user may zoom in and zoom out when utilizing the topology window to get a better, more defined view of the configurations.

Single IP Settings

All switches are set as Candidate (CaS) switches as their factory default configuration and Single IP Management will be disabled.

To enable SIM for the Switch using the Web interface, click **Configuration > Single IP Managemnet > Single IP Settings** which will reveal the following window:

Figure 2 - 41. Single IP Settings window (disabled)

Use the drop-down menus to change the SIM State to *Enabled*, the Role State to *Commander*, and then fill in the Group Name field. Click **Apply** to let the changes take effect.

Figure 2 - 42. Single IP Settings window (enabled)

The following parameters can be set:

Parameters	Description
SIM State	Use the pull-down menu to either enable or disable the SIM state on the Switch. *Disabled* will render all SIM functions on the Switch inoperable.
Role State	Use the pull-down menu to change the SIM role of the Switch. The two choices are: *Candidate* - A Candidate Switch (CaS) is not the member of a SIM group but is connected to a Commander Switch. This is the default setting for the SIM role. *Commander* - Choosing this parameter will make the Switch a Commander Switch (CS). The user may join other switches to this Switch, over Ethernet, to be part of its SIM group. Choosing this option will also enable the Switch to be configured for SIM.
Group Name	The user may enter a name for the group.
Discovery Interval (30-90)	The user may set the discovery protocol interval, in seconds that the Switch will send out discovery packets. Returning information to a Commander Switch will include information about other switches connected to it. (Ex. MS, CaS). The user may set the Discovery Interval from *30* to *90* seconds.
Hold Time Count (100-255)	This parameter may be set for the time, in seconds the Switch will hold information sent to it from other switches, utilizing the Discovery Interval. The user may set the hold time from *100* to *255* seconds.

Click **Apply** to implement the settings.

After enabling the Switch to be a Commander Switch (CS), the **Single IP Management** folder will then contain four added links to aid the user in configuring SIM through the Web, including **Topology**, **Firmware Upgrade** and **Configuration File Backup/Restore** and **Upload Log File**.

Topology

The **Topology** window will be used to configure and manage the Switch within the SIM group and requires Java script to function properly on your computer.

The Java Runtime Environment on your server should initiate and lead you to the **Topology** window:

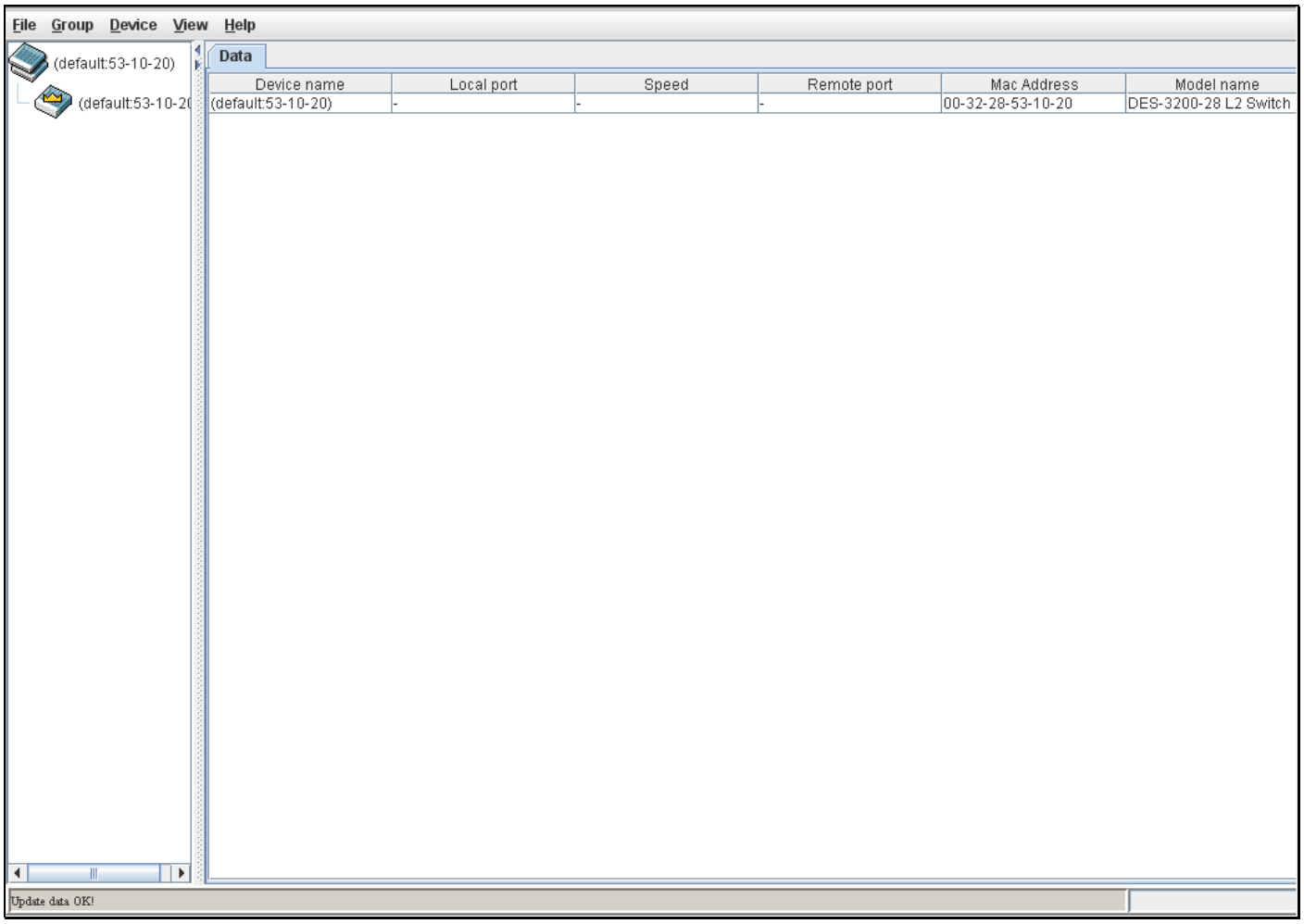


Figure 2 - 43. Topology window

The **Topology** window holds the following information under the **Data** tab:

Parameter	Description
Device Name	This field will display the Device Name of the switches in the SIM group configured by the user. If no Device Name is configured by the name, it will be given the name default and tagged with the last six digits of the MAC Address to identify it.
Remote Port	Displays the number of the physical port on the MS or CaS that the CS is connected to. The CS will have no entry in this field.
Speed	Displays the connection speed between the CS and the MS or CaS.
Local Port	Displays the number of the physical port on the CS that the MS or CaS is connected to. The CS will have no entry in this field.
MAC Address	Displays the MAC address of the corresponding Switch.

Model Name	Displays the full model name of the corresponding Switch.

To view the Topology Map, click the **View** menu in the toolbar and then **Topology**, which will produce the following window. The Topology View will refresh itself periodically (20 seconds by default).

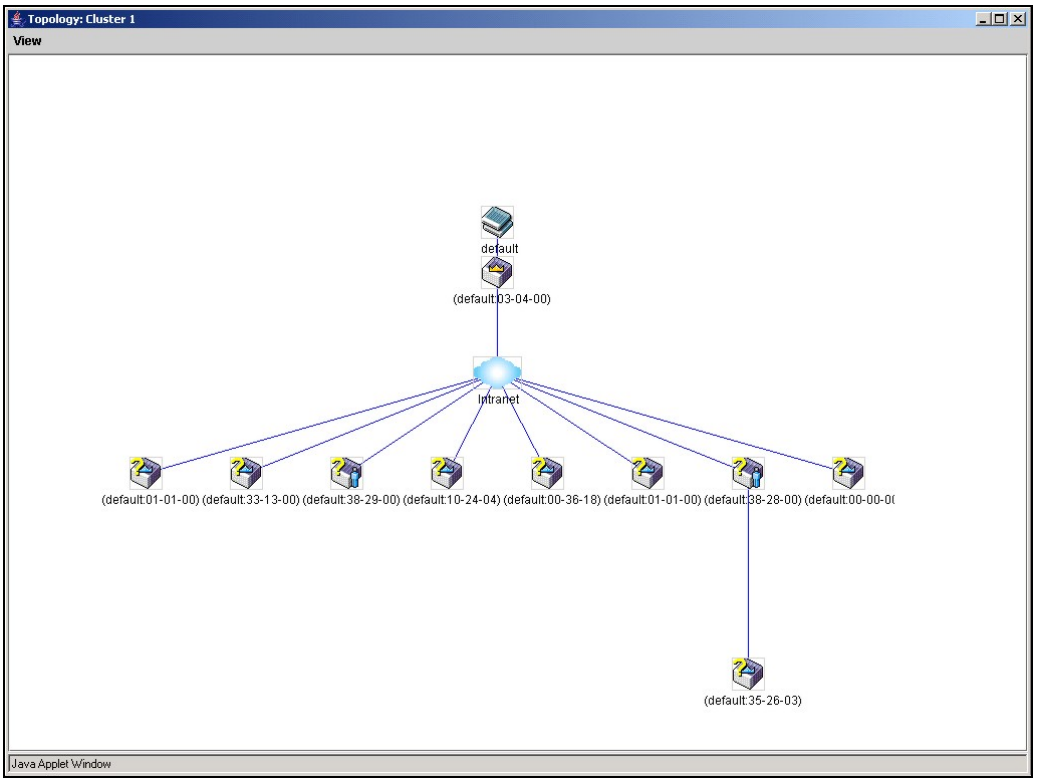


Figure 2 - 44. Topology view

This window will display how the devices within the Single IP Management Group are connected to other groups and devices. Possible icons in this window are as follows:

Icon	Description
	Group
	Layer 2 commander switch
	Layer 3 commander switch
	Commander switch of other group
	Layer 2 member switch.
	Layer 3 member switch
	Member switch of other group
	Layer 2 candidate switch
	Layer 3 candidate switch
	Unknown device

	Non-SIM devices

Tool Tips

In the Topology view window, the mouse plays an important role in configuration and in viewing device information. Setting the mouse cursor over a specific device in the topology window (tool tip) will display the same information about a specific device as the Tree view does. See the window below for an example:

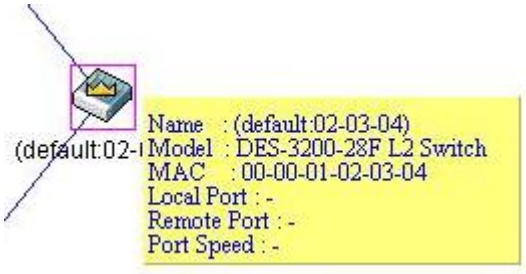


Figure 2 - 45. Device Information Utilizing the Tool Tip

Setting the mouse cursor over a line between two devices will display the connection speed between the two devices, as shown below:

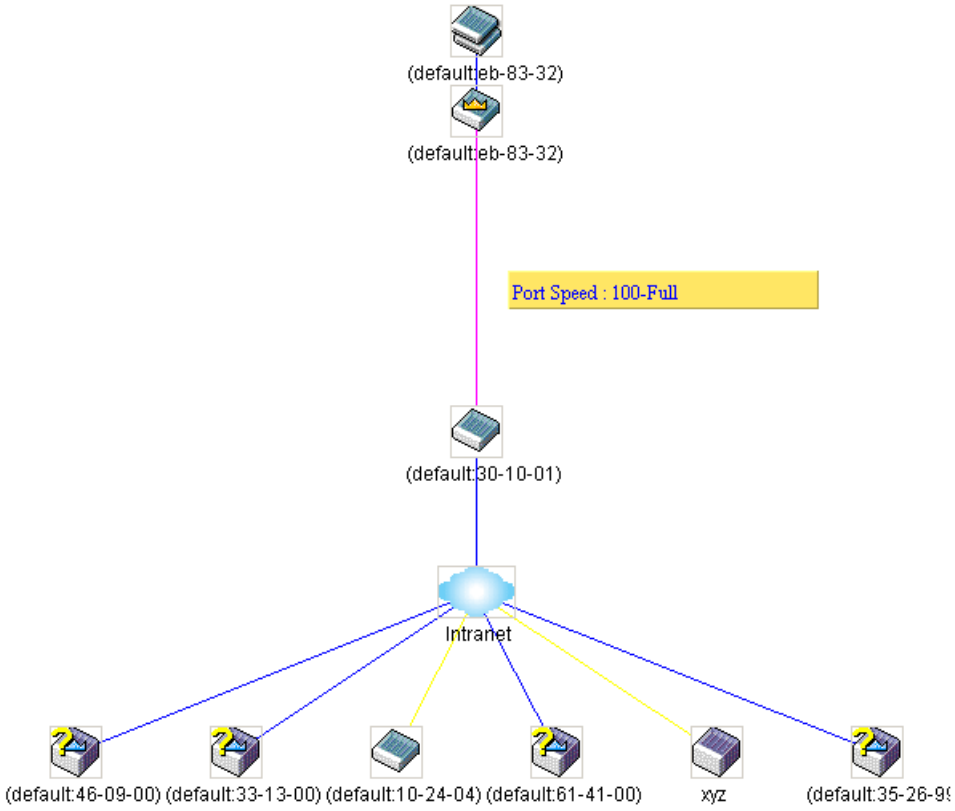


Figure 2 - 46. Port Speed Utilizing the Tool Tip

Right-Click

Right-clicking on a device will allow the user to perform various functions, depending on the role of the Switch in the SIM group and the icon associated with it.

Group Icon

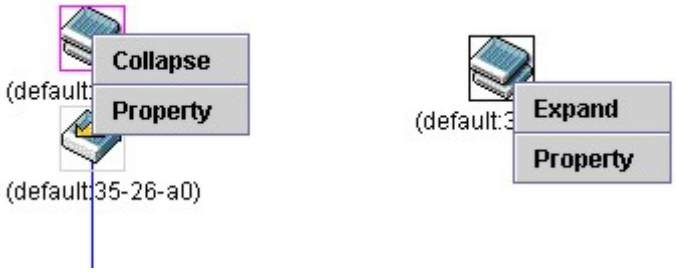


Figure 2 - 47. Right-Clicking a Group Icon

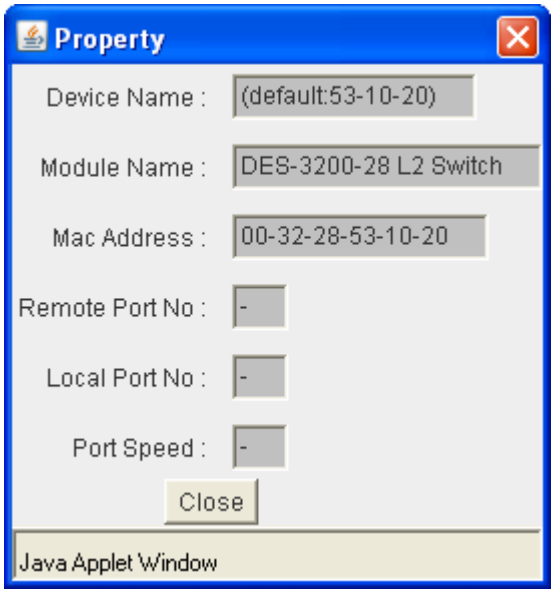


Figure 2 - 48. Property window

This window holds the following information:

Parameter	Description
Device Name	This field will display the Device Name of the switches in the SIM group configured by the user. If no Device Name is configured by the name, it will be given the name default and tagged with the last six digits of the MAC Address to identify it.
Module Name	Displays the full module name of the switch that was right-clicked.
MAC Address	Displays the MAC Address of the corresponding Switch.
Local Port No.	Displays the number of the physical port on the CS that the MS or CaS is connected to. The CS will have no entry in this field.
Remote Port No.	Displays the number of the physical port on the MS or CaS that the CS is connected to. The CS will have no entry in this field.
Port Speed	Displays the connection speed between the CS and the MS or CaS

Click **Close** to close the **Property** window.

Commander Switch Icon

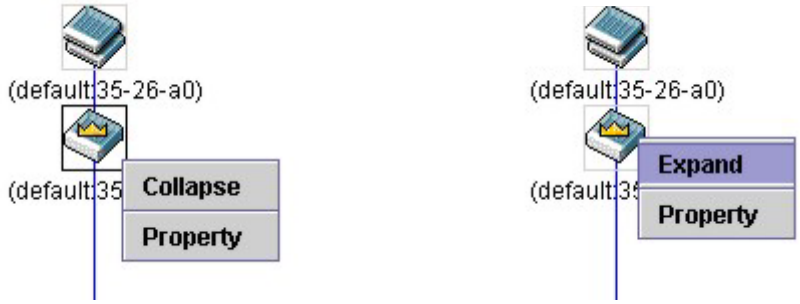


Figure 2 - 49. Right-Clicking a Commander Icon

The following options may appear for the user to configure:

- **Collapse** - To collapse the group that will be represented by a single icon.
- **Expand** - To expand the SIM group, in detail.
- **Property** - To pop up a window to display the group information.

Member Switch Icon

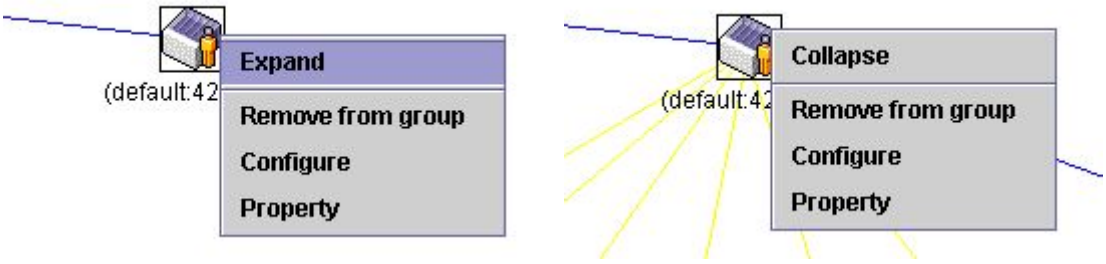


Figure 2 - 50. Right-Clicking a Member icon

The following options may appear for the user to configure:

- **Collapse** - To collapse the group that will be represented by a single icon.
- **Expand** - To expand the SIM group, in detail.
- **Remove from group** - Remove a member from a group.
- **Configure** - Launch the web management to configure the Switch.
- **Property** - To pop up a window to display the device information.

Candidate Switch Icon

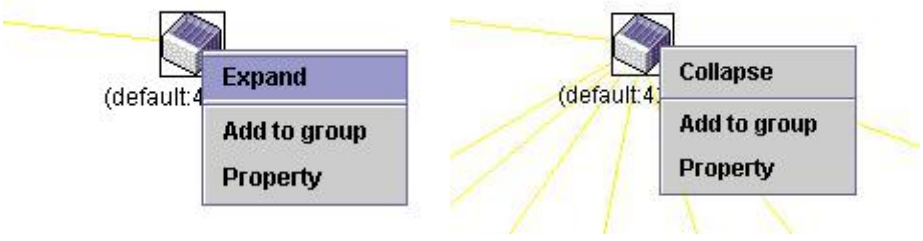


Figure 2 - 51. Right-Clicking a Candidate icon

The following options may appear for the user to configure:

- **Collapse** - To collapse the group that will be represented by a single icon.
- **Expand** - To expand the SIM group in detail.

- **Add to group** - Add a candidate to a group. Clicking this option will reveal the following dialog for the user to enter a password for authentication from the Candidate Switch before being added to the SIM group. Click **OK** to enter the password or **Cancel** to exit the window.

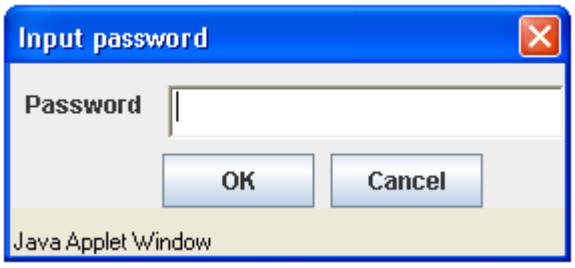


Figure 2 - 52. Input password window

- **Property** - To pop up a window to display the device information.

Menu Bar

The **Single IP Management** window contains a menu bar for device configurations, as seen below.

Figure 2 - 53. Menu Bar of the Topology View

The five menus on the menu bar are as follows.

File

- **Print Setup** - Will set the default printer properties.
- **Print Topology** - Will print the topology map.
- **Preference** - Will set display properties, such as polling interval, and the views to open at SIM startup.

Group

- **Add to group** - Add a candidate to a group. Clicking this option will reveal the following dialog for the user to enter a password for authentication from the Candidate Switch before being added to the SIM group. Click **OK** to enter the password or **Cancel** to exit the window.

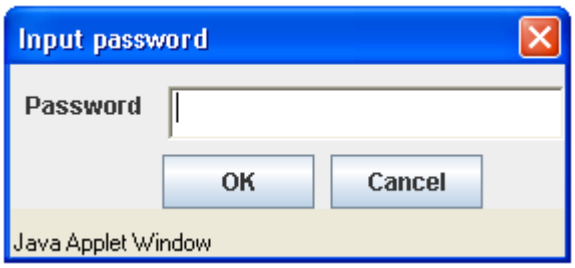


Figure 2 - 54. Input password window

- **Remove from Group** - Remove an MS from the group.

Device

- **Configure** - Will open the web manager for the specific device.

View

- **Refresh** - Update the views with the latest status.
- **Topology** - Display the Topology view.

Help

- **About** - Will display the SIM information, including the current SIM version.

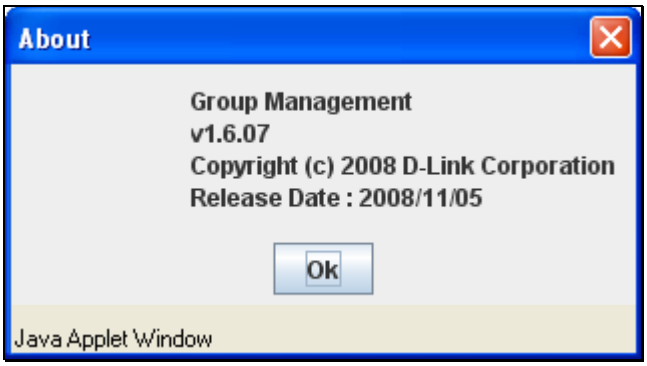


Figure 2 - 55. About window

Firmware Upgrade

This window is used to upgrade firmware from the Commander Switch to the Member Switch. Member Switches will be listed in the table and will be specified by ID and Port (port on the CS where the MS resides), MAC Address, Model Name and Firmware Version. To specify a certain Switch for firmware download, click its corresponding check box under the Port heading. To update the firmware, enter the Server IP Address where the firmware resides and enter the Path/Filename of the firmware. Click **Download** to initiate the file transfer.

To access the following window, click **Configuration > Single IP Management > Firmware Upgrade**:

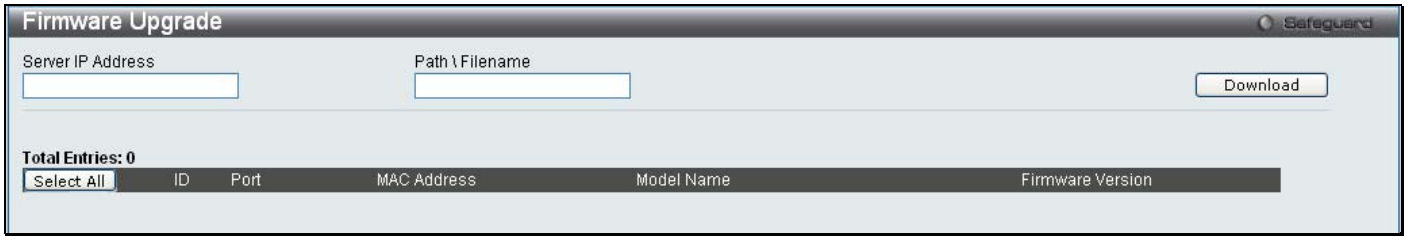


Figure 2 - 56. Firmware Upgrade window

Configuration File Backup/Restore

This window is used to upgrade configuration files from the Commander Switch to the Member Switch using a TFTP server. Member Switches will be listed in the table and will be specified by ID, Port (port on the CS where the MS resides), MAC Address, Model Name and Firmware Version. To update the configuration file, enter the Server IP Address where the file resides and enter the Path/Filename of the configuration file. Click **Restore** to initiate the file transfer from a TFTP server to the Switch. Click **Backup** to backup the configuration file to a TFTP server. To access the following window, click **Configuration > Single IP Management > Configuration File Backup/Restore**:

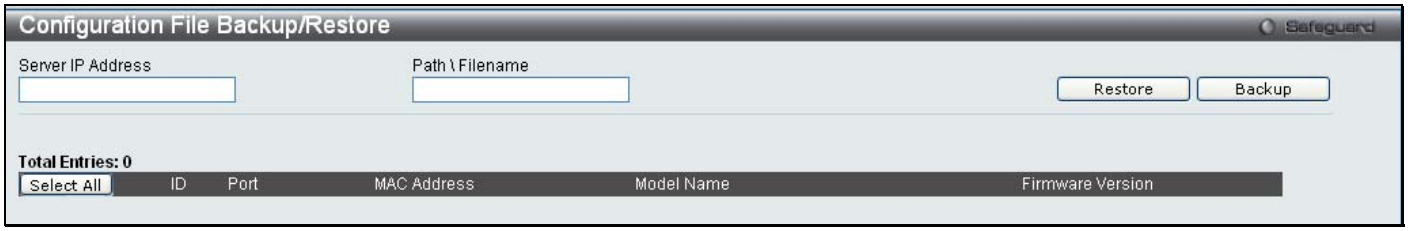


Figure 2 - 57. Configuration File Backup/Restore window

Upload Log File

The following window is used to upload log files from SIM member switches to a specified PC. To upload a log file, enter the Server IP address of the SIM member switch and then enter a Path\Filename on your PC where you wish to save this file. Click **Upload** to initiate the file transfer. To view this window click **Configuration > Single IP Management > Upload Log File**

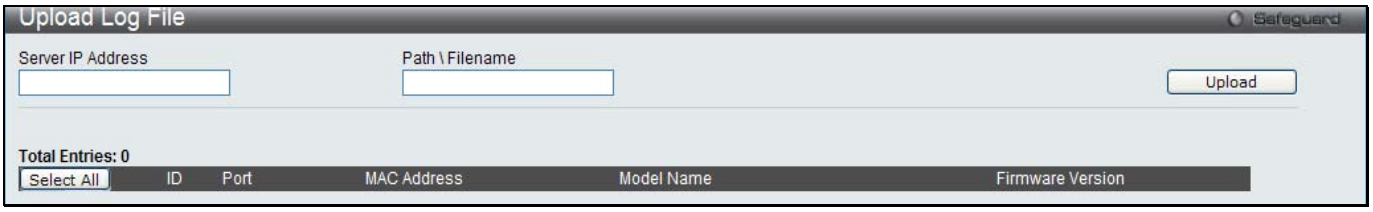


Figure 2 - 58. Upload Log File window

Gratuitous ARP

An ARP announcement (also known as Gratuitous ARP) is a packet (usually an ARP Request) containing a valid SHA and SPA for the host which sent it, with TPA equal to SPA. Such a request is not intended to solicit a reply, but merely updates the ARP caches of other hosts which receive the packet.
This is commonly done by many operating systems on startup, and helps to resolve problems which would otherwise occur if, for example, a network card had recently been changed (changing the IP address to MAC address mapping) and other hosts still had the old mapping in their ARP cache.

Gratuitous ARP Global Settings

To view this window, click **Configuration > Gratuitous ARP > Gratuitous ARP Global Settings**:

Figure 2 - 59. Gratuitous ARP Global Settings window

The following fields can be configured:

Parameter	Description
Send On IP Interface Status Up	This is used to enable or disable the sending of gratuitous ARP request packets while an IP interface comes up. This is used to automatically announce the interface's IP address to other nodes. By default, the state is *Enabled*.
Send On Duplicate IP Detected	This is used to enable or disable the sending of gratuitous ARP request packets while a duplicate IP is detected. By default, the state is *Enabled*. Duplicate IP detected means that the system received an ARP request packet that is sent by an IP address that matches the system's own IP address.
Gratuitous ARP Learning	This is used to enable or disable updating ARP cache based on the received gratuitous ARP packet. If a switch receives a gratuitous ARP packet, it should add or update the ARP entry. This is *Enabled* by default.

Once you have made the desired gratuitous ARP setting changes, click **Apply**.

Gratuitous ARP Settings

This window allows you to have more detailed settings for the Gratuitous ARP.

To view this window, click **Configuration > Gratuitous ARP > Gratuitous ARP Settings**:

Figure 2 - 60. Gratuitous ARP Settings window

The following fields can be set or viewed:

Parameter	Description
Gratuitous ARP Trap/Log	
Trap	The switch can trap IP conflict events to inform the administrator. By default, trap is *Disabled*.
Log	The switch can log IP conflict events to inform the administrator. By default, Log is *Enabled*.
IP Interface Name	Displays the name of the interface that is being edited.
Gratuitous ARP Periodical Send Interval	
IP Interface Name	Displays the name of the interface that is being edited.
Interval Time (0-65535)	This is used to configure the interval for the periodical sending of gratuitous ARP request packets. By default, the interval is *0*.

Click **Apply** to implement changes made.

ARP Spoofing Prevention Settings

ARP spoofing, also known as ARP poisoning, is a method to attack an Ethernet network which may allow an attacker to sniff data frames on a LAN, modify the traffic, or stop the traffic altogether (known as a Denial of Service - DoS attack). The principle of ARP spoofing is to send the fake, or spoofed ARP messages to an Ethernet network. Generally, the aim is to associate the attacker's or random MAC address with the IP address of another node (such as the default gateway). Any traffic meant for that IP address would be mistakenly re-directed to the node specified by the attacker.

To prevent ARP spoofing attack, the switch uses Packet Content ACL to block the invalid ARP packets which contain faked gateway's MAC and IP binding.

To view this window, click **Configuration** > **ARP Spoofing Prevention Settings** as shown below:

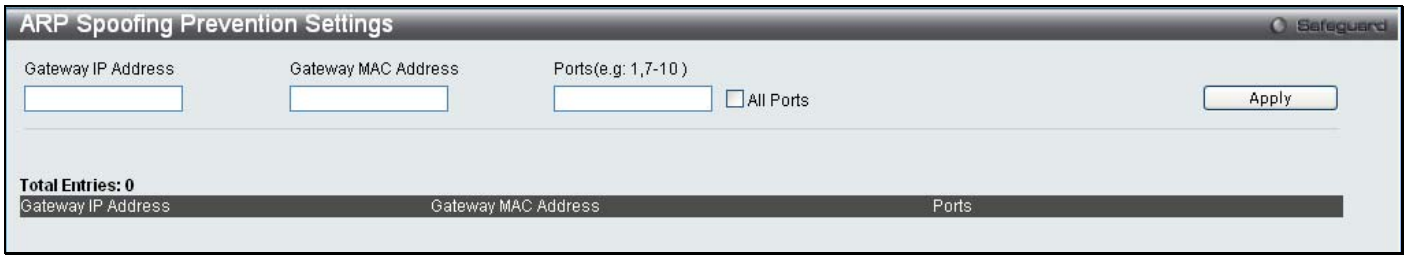


Figure 2 - 61. ARP Spoofing Prevention Settings window

The following fields can be set or viewed:

Parameter	Description
Gateway IP Address	Enter the IP address of the gateway.
Gateway MAC Address	Enter the MAC address of the gateway.
Ports (e.g.: 1, 7-10)	Specify the switch ports for which to configure the ARP Spoofing Prevention settings. Tick the All Ports check box to configure this entry for all ports on the Switch.

Section 3

L2 Features

Jumbo Frame
802.1Q Static VLAN
Q-in-Q
802.1v Protocol VLAN
VLAN Trunk Settings
GVRP Settings
Asymmetric VLAN Settings
MAC-based VLAN Settings
PVID Auto Assign Settings
Port Trunking
LACP Port Settings
Traffic Segmentation
BPDU Tunneling Settings
IGMP Snooping
MLD Snooping Settings
Port Mirror
Loopback Detection Settings
Spanning Tree
Forwarding & Filtering
LLDP

The following section will aid the user in configuring Layer 2 functions for the Switch. The Switch includes various functions all discussed in detail in the following section.

Jumbo Frame

This window will enable or disable the Jumbo Frame function on the Switch. The default is Enabled. When Enabled, jumbo frames (frames larger than the standard Ethernet frame size of 1536 bytes) with a maximum size of 2048 bytes can be transmitted by the Switch.

To view this window, click **L2 Features > Jumbo Frame**:

Figure 3 - 1. Jumbo Frame window

Click **Apply** to implement changes made.

VLANs

Understanding IEEE 802.1p Priority

Priority tagging is a function defined by the IEEE 802.1p standard designed to provide a means of managing traffic on a network where many different types of data may be transmitted simultaneously. It is intended to alleviate problems associated with the delivery of time critical data over congested networks. The quality of applications that are dependent on such time critical data, such as video conferencing, can be severely and adversely affected by even very small delays in transmission.

Network devices that are in compliance with the IEEE 802.1p standard have the ability to recognize the priority level of data packets. These devices can also assign a priority label or tag to packets. Compliant devices can also strip priority tags from packets. This priority tag determines the packet's degree of expeditiousness and determines the queue to which it will be assigned.

Priority tags are given values from 0 to 7 with 0 being assigned to the lowest priority data and 7 assigned to the highest. The highest priority tag 7 is generally only used for data associated with video or audio applications, which are sensitive to even slight delays, or for data from specified end users whose data transmissions warrant special consideration.

The Switch allows you to further tailor how priority tagged data packets are handled on your network. Using queues to manage priority tagged data allows you to specify its relative priority to suit the needs of your network. There may be circumstances where it would be advantageous to group two or more differently tagged packets into the same queue. Generally, however, it is recommended that the highest priority queue, Queue 7, be reserved for data packets with a priority value of 7. Packets that have not been given any priority value are placed in Queue 0 and thus given the lowest priority for delivery.

Strict mode and weighted round robin system are employed on the Switch to determine the rate at which the queues are emptied of packets. The ratio used for clearing the queues is 4:1. This means that the highest priority queue, Queue 7, will clear 4 packets for every 1 packet cleared from Queue 0.

Remember, the priority queue settings on the Switch are for all ports, and all devices connected to the Switch will be affected. This priority queuing system will be especially beneficial if your network employs switches with the capability of assigning priority tags.

VLAN Description

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLANs can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLANs also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLANs can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.

Notes About VLANs

No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLANs without a network device performing a routing function between the VLANs.

The Switch supports IEEE 802.1Q VLANs and Port-Based VLANs. The port untagging function can be used to remove the 802.1Q tag from packet headers to maintain compatibility with devices that are tag-unaware.

The Switch's default is to assign all ports to a single 802.1Q VLAN named "default."

The "default" VLAN has a VID = 1.

The member ports of Port-based VLANs may overlap, if desired.

IEEE 802.1Q VLANs

Some relevant terms:

- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.
- **Ingress port** - A port on a switch where packets are flowing into the Switch and VLAN decisions must be made.
- **Egress port** - A port on a switch where packets are flowing out of the Switch, either to another switch or to an end station, and tagging decisions must be made.

IEEE 802.1Q (tagged) VLANs are implemented on the Switch. 802.1Q VLANs require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLANs allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources.

VLANs can also provide a level of security to your network. IEEE 802.1Q VLANs will only deliver packets between stations that are members of the VLAN.

Any port can be configured as either tagging or untagging. The untagging feature of IEEE 802.1Q VLANs allows VLANs to work with legacy switches that don't recognize VLAN tags in packet headers. The tagging feature allows VLANs to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

The IEEE 802.1Q standard restricts the forwarding of untagged packets to the VLAN of which the receiving port is a member.

The main characteristics of IEEE 802.1Q are as follows:

- Assigns packets to VLANs by filtering.
- Assumes the presence of a single global spanning tree.
- Uses an explicit tagging scheme with one-level tagging.
- 802.1Q VLAN Packet Forwarding
- Packet forwarding decisions are made based upon the following three types of rules:
- Ingress rules - rules relevant to the classification of received frames belonging to a VLAN.
- Forwarding rules between ports - decides whether to filter or forward the packet.
- Egress rules - determines if the packet must be sent tagged or untagged.

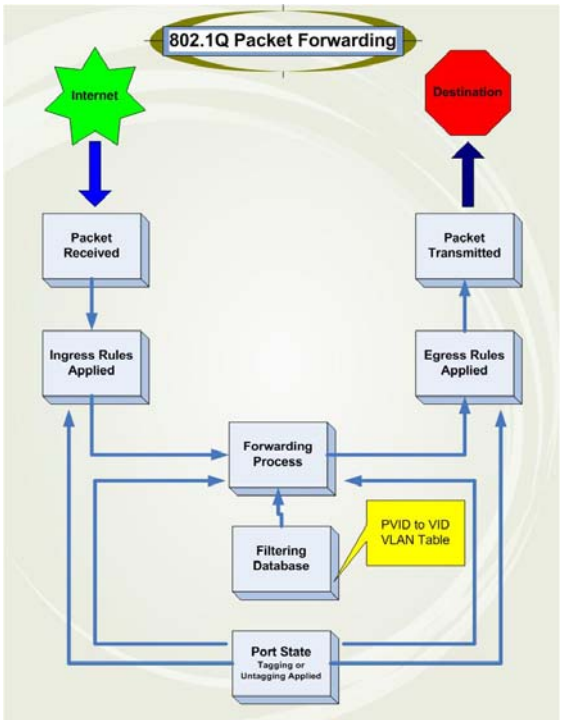


Figure 3 - 2. IEEE 802.1Q Packet Forwarding

802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of 0x8100 in the EtherType field. When a packet's EtherType field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of three bits of user priority, one bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and twelve bits of VLAN ID (VID). The three bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is twelve bits long, 4094 unique VLANs can be identified.

The tag is inserted into the packet header making the entire packet longer by four octets. All of the information originally contained in the packet is retained.

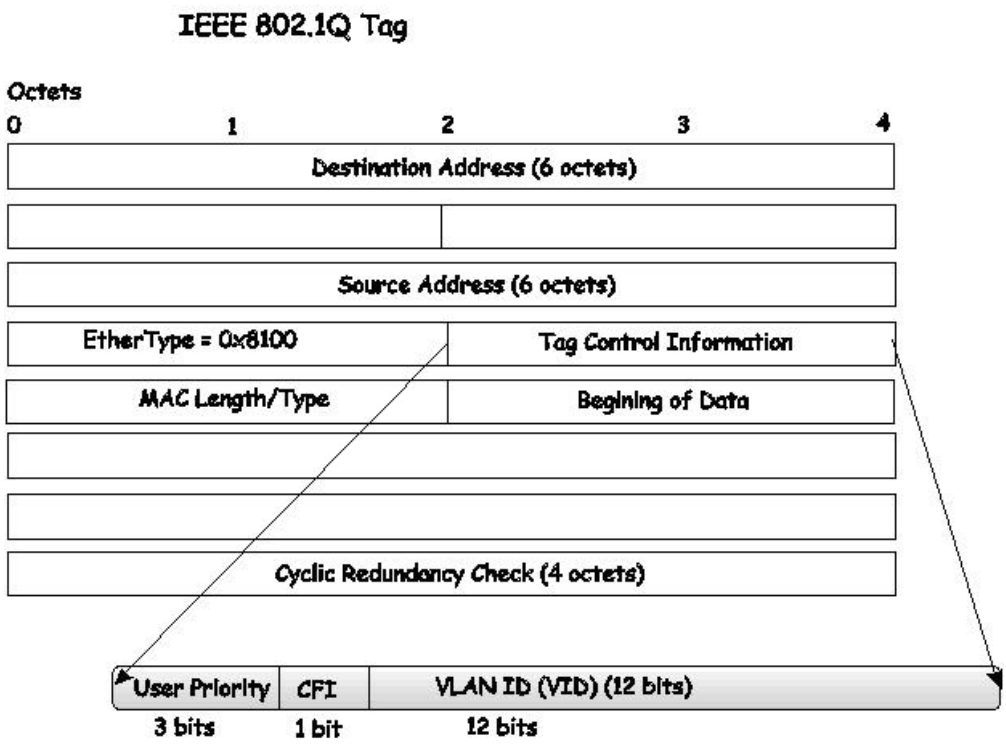


Figure 3 - 3. IEEE 802.1Q Tag

The EtherType and VLAN ID are inserted after the MAC source address, but before the original EtherType/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

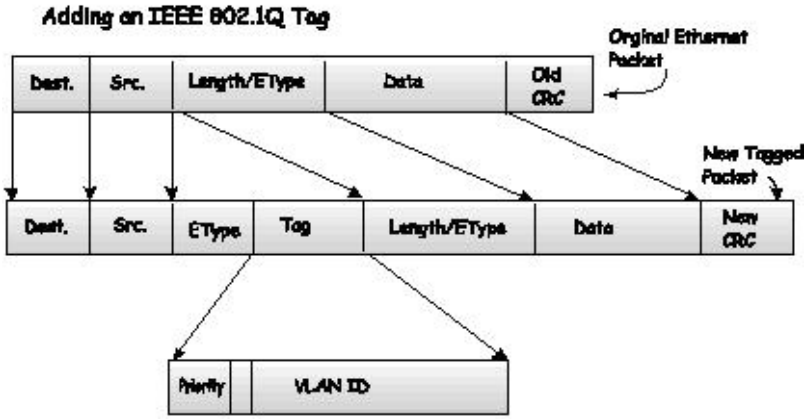


Figure 3 - 4. Adding an IEEE 802.1Q Tag

Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLANs to span network devices (and indeed, the entire network, if all network devices are 802.1Q compliant).

Unfortunately, not all network devices are 802.1Q compliant. These devices are referred to as tag-unaware. 802.1Q devices are referred to as tag-aware.

Prior to the adoption of 802.1Q VLANs, port-based and MAC-based VLANs were in common use. These VLANs relied upon a Port VLAN ID (PVID) to forward packets. A packet received on a given port would be assigned that port's PVID and then be forwarded to the port that corresponded to the packet's destination address (found in the Switch's forwarding table). If the PVID of the port that received the packet is different from the PVID of the port that is to transmit the packet, the Switch will drop the packet.

Within the Switch, different PVIDs mean different VLANs (remember that two VLANs cannot communicate without an external router). So, VLAN identification based upon the PVIDs cannot create VLANs that extend outside a given switch (or switch stack).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the Switch. If no VLANs are defined on the Switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLANs are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet-forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVIDs within the Switch to VIDs on the network. The Switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VIDs are different, the Switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VIDs as the Switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted - should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Tagging and Untagging

Every port on an 802.1Q compliant switch can be configured as tagging or untagging.

Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into and out of it. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. Other 802.1Q compliant devices on the network to make packet-forwarding decisions can then use the VLAN information in the tag.

Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into and out of those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Ingress Filtering

A port on a switch where packets are flowing into the Switch and VLAN decisions must be made is referred to as an ingress port. If ingress filtering is enabled for a port, the Switch will examine the VLAN information in the packet header (if present) and decide whether or not to forward the packet.

If the packet is tagged with VLAN information, the ingress port will first determine if the ingress port itself is a member of the tagged VLAN. If it is not, the packet will be dropped. If the ingress port is a member of the 802.1Q VLAN, the Switch then determines if the destination port is a member of the 802.1Q VLAN. If it is not, the packet is dropped. If the destination port is a member of the 802.1Q VLAN, the packet is forwarded and the destination port transmits it to its attached network segment.

If the packet is not tagged with VLAN information, the ingress port will tag the packet with its own PVID as a VID (if the port is a tagging port). The switch then determines if the destination port is a member of the same VLAN (has the same VID) as the ingress port. If it does not, the packet is dropped. If it has the same VID, the packet is forwarded and the destination port transmits it on its attached network segment.

This process is referred to as ingress filtering and is used to conserve bandwidth within the Switch by dropping packets that are not on the same VLAN as the ingress port at the point of reception. This eliminates the subsequent processing of packets that will just be dropped by the destination port.

Default VLANs

The Switch initially configures one VLAN, VID = 1, called "default." The factory default setting assigns all ports on the Switch to the "default." As new VLANs are configured in Port-based mode, their respective member ports are removed from the "default."

Packets cannot cross VLANs. If a member of one VLAN wants to connect to another VLAN, the link must be through an external router.

NOTE: If no VLANs are configured on the Switch, then all packets will be forwarded to any destination port. Packets with unknown source addresses will be flooded to all ports. Broadcast and multicast packets will also be flooded to all ports.

An example is presented below:

VLAN Name	VID	Switch Ports
System (default)	1	5, 6, 7, 8, 21, 22, 23, 24
Engineering	2	9, 10, 11, 12
Marketing	3	13, 14, 15, 16
Finance	4	17, 18, 19, 20
Sales	5	1, 2, 3, 4

Table 3 - 1. VLAN Example - Assigned Ports

Port-based VLANs

Port-based VLANs limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department.

On port-based VLANs, NICs do not need to be able to identify 802.1Q tags in packet headers. NICs send and receive normal Ethernet packets. If the packet's destination lies on the same segment, communications take place using normal Ethernet protocols. Even though this is always the case, when the destination for a packet lies on another switch port, VLAN considerations come into play to decide if the packet gets dropped by the Switch or delivered.

VLAN Segmentation

Take for example a packet that is transmitted by a machine on Port 1 that is a member of VLAN 2. If the destination lies on another port (found through a normal forwarding table lookup), the Switch then looks to see if the other port (Port 10) is a member of VLAN 2 (and can therefore receive VLAN 2 packets). If Port 10 is not a member of VLAN 2, then the packet will be dropped by the Switch and will not reach its destination. If Port 10 is a member of VLAN 2, the packet will go through. This selective forwarding feature based on VLAN criteria is how VLANs segment networks. The key point being that Port 1 will only transmit on VLAN 2.

Network resources can be shared across VLANs. This is achieved by setting up overlapping VLANs. That is ports can belong to more than one VLAN group. For example, by setting VLAN 1 members to ports 1, 2, 3 and 4 and VLAN 2 members to ports 1, 5, 6 and 7, Port 1 will belong to two VLAN groups. Ports 8, 9 and 10 are not configured to any VLAN group. This means ports 8, 9 and 10 are in the same VLAN group.

VLAN and Trunk Groups

The members of a trunk group have the same VLAN setting. Any VLAN setting on the members of a trunk group will apply to the other member ports.

NOTE: In order to use VLAN segmentation in conjunction with port trunk groups, you can first set the port trunk group(s), and then you may configure VLAN settings. If you wish to change the port trunk grouping with VLANs already in place, you will not need to reconfigure the VLAN settings after changing the port trunk group settings. VLAN settings will automatically change in conjunction with the change of the port trunk group settings.

Q-in-Q VLANs

Q-in-Q VLANs (also sometimes referred to as double VLANs) allow network providers to expand their VLAN configurations to place customer VLANs within a larger inclusive VLAN, which adds a new layer to the VLAN configuration. This basically lets large ISP's create L2 Virtual Private Networks and also create transparent LANs for their customers, which will connect two or more customer LAN points without over-complicating configurations on the client's side. Not only will over-complication be avoided, but also now the administrator has over 4000 VLANs in which

over 4000 VLANs can be placed, therefore greatly expanding the VLAN network and enabling greater support of customers utilizing multiple VLANs on the network.

Q-in-Q VLANs are basically VLAN tags placed within existing IEEE 802.1Q VLANs which we will call SPVIDs (Service Provider VLAN IDs). These VLANs are marked by a TPID (Tagged Protocol ID), configured in hex form to be encapsulated within the VLAN tag of the packet. This identifies the packet as double-tagged and segregates it from other VLANs on the network, therefore creating a hierarchy of VLANs within a single packet.

Here is an example Q-in-Q VLAN tagged packet:

Destination Address	Source Address	SPVLAN (TPID + Service Provider VLAN Tag)	802.1Q CEVLAN Tag (TPID + Customer VLAN Tag)	Ether Type	Payload

Consider the example below:

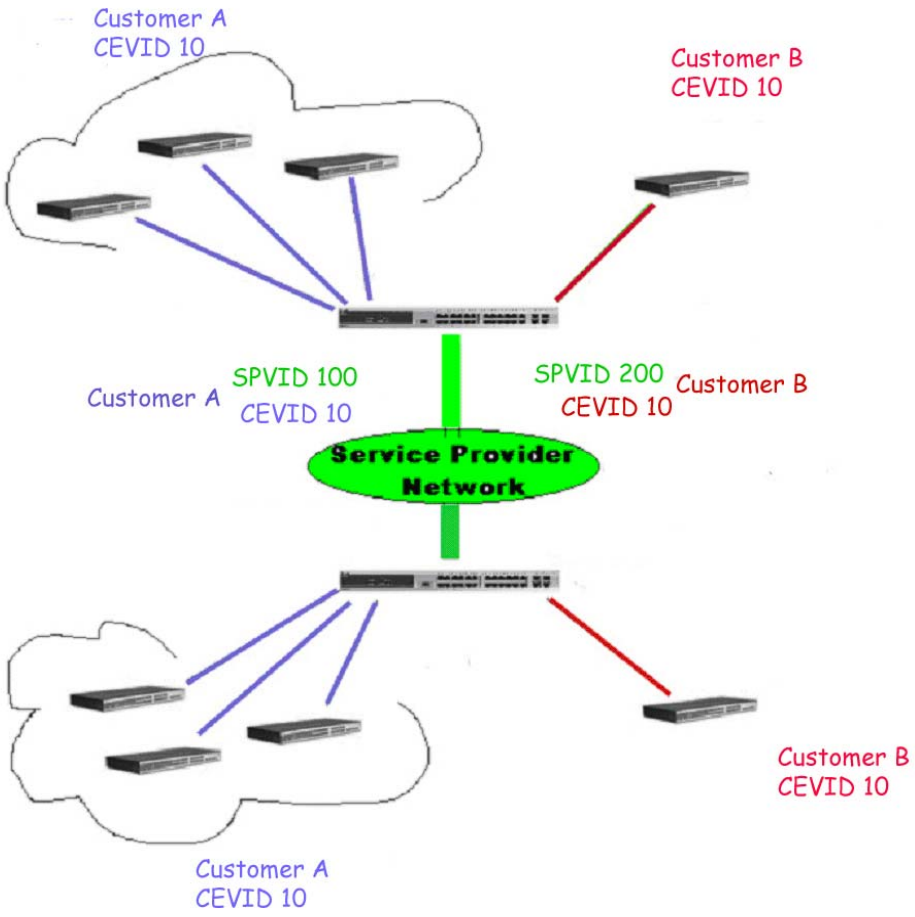


Figure 3 - 5. Q-in-Q VLAN Example

In this example, the Service Provider Access Network switch (Provider edge switch) is the device creating and configuring Q-in-Q VLANs with different SPVIDs for specific customers (say Customer A and Customer B). Both CEVLANs (Customer VLANs), CEVLAN 10 are tagged with the SPVID 100 (for Customer A) or SPVID 200 (for Customer B) on the Service Provider Access Network, thus being a member of two VLANs on the Service Provider's network. In this way, the Customer can retain their normal VLAN ID's and the Service Provider can seperate multiple Customer VLANs using SPVLANs, thus greatly regulating traffic and routing on the Service Provider switch. This information is then routed to the Service Provider's main network and regarded there as one VLAN, with one set of protocols and one routing behavior.

Regulations for Q-in-Q VLANs

Some rules and regulations apply with the implementation of the Q-in-Q VLAN procedure.

1. All ports must be configured for the SPVID and its corresponding TPID on the Service Provider's edge switch.

2. All ports must be configured as Access Ports or Uplink ports. Access ports can only be Ethernet ports while Uplink ports must be Gigabit ports.
3. Provider Edge switches must allow frames of at least 1522 bytes or more, due to the addition of the SPVID tag.
4. Access Ports must be an un-tagged port of the service provider VLANs. Uplink Ports must be a tagged port of the service provider VLANs.
5. The switch cannot have both Q-in-Q and normal VLANs co-existing. Once the change of VLAN is made, all Access Control lists are cleared and must be reconfigured.
6. Before Q-in-Q VLANs are enabled, users need to disable STP and GVRP manually.
7. All packets sent from the CPU to the Access ports must be untagged.

802.1Q Static VLAN

This window lists all previously configured VLANs by VLAN ID and VLAN Name.

To view this window, click **L2 Features > 802.1Q Static VLAN**:

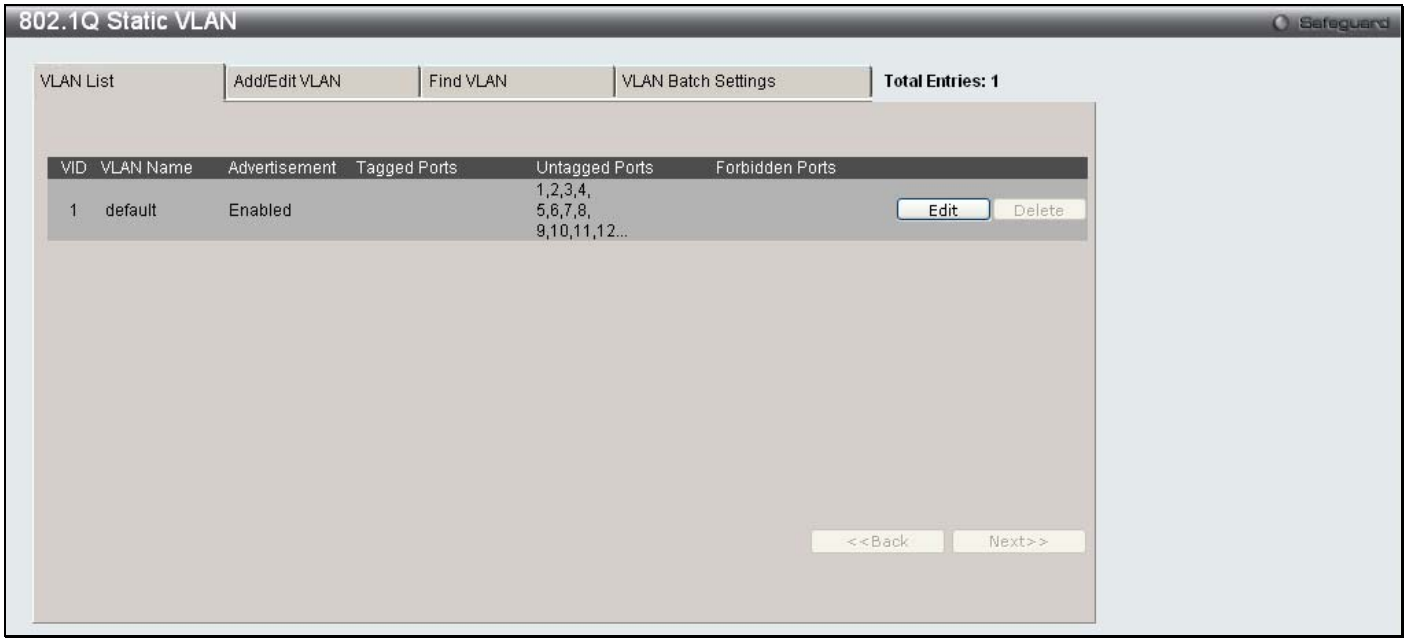


Figure 3 - 6. 802.1Q Static VLAN window - VLAN List tab

To create a new 802.1Q VLAN entry, click the **Add/Edit VLAN** tab at the top of the window. A new tab will appear, as shown in the first figure on the next page, to configure the port settings and to assign a unique name and number to the new VLAN.

To edit an existing 802.1Q VLAN entry, click the **Edit** button next to the corresponding VLAN entry above. A new tab will appear, as shown in the second figure on the next page.

See the table on the next page for a description of the parameters of the **802.1Q Static VLAN** window's **Add/Edit VLAN** tab.

NOTE: After all IP interfaces are set for configurations, VLANs on the Switch can be routed without any additional steps.

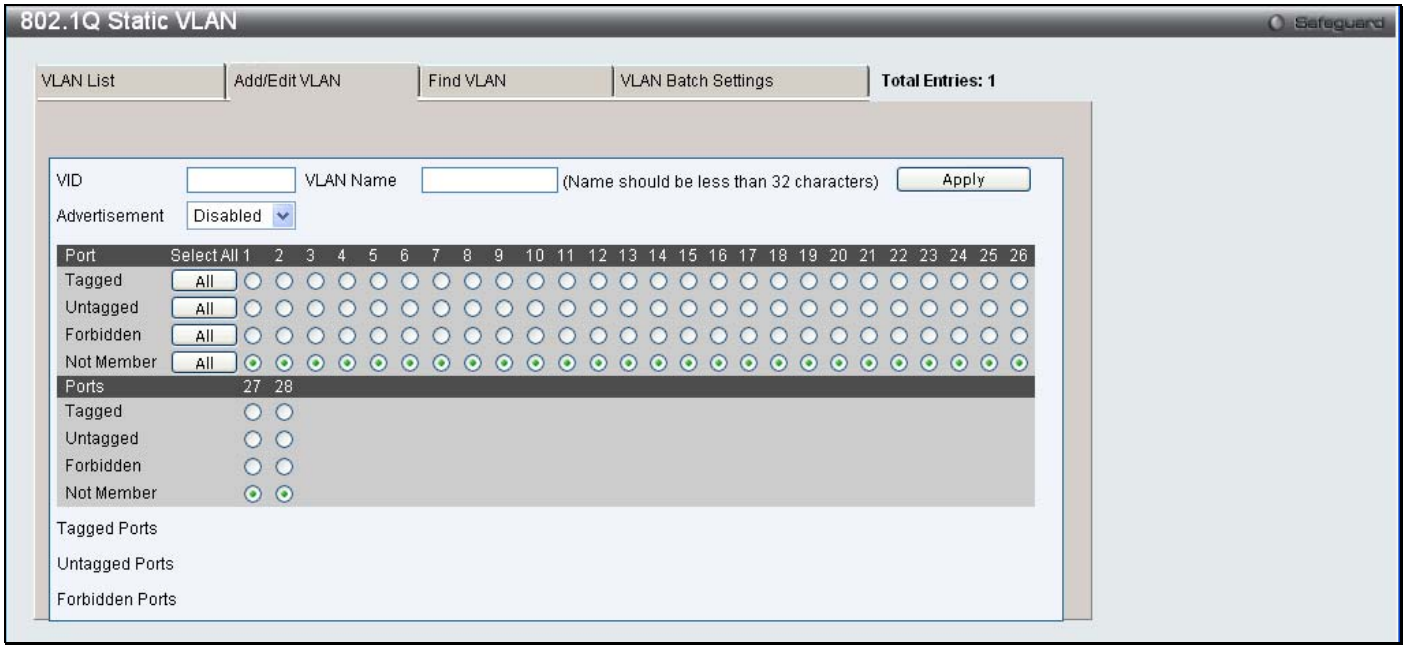


Figure 3 - 7. 802.1Q Static VLAN window – Add/Edit VLAN tab (Add)

To return to the initial **802.1Q Static VLAN** window, click the **VLAN List** tab at the top of the window. To change an existing 802.1Q static VLAN entry, click the corresponding **Edit** button. A new window will appear to configure the port settings and to assign a unique name and number to the new VLAN. See the table below for a description of the parameters in the new window.

NOTE: The Switch supports up to 4k static VLAN entries.

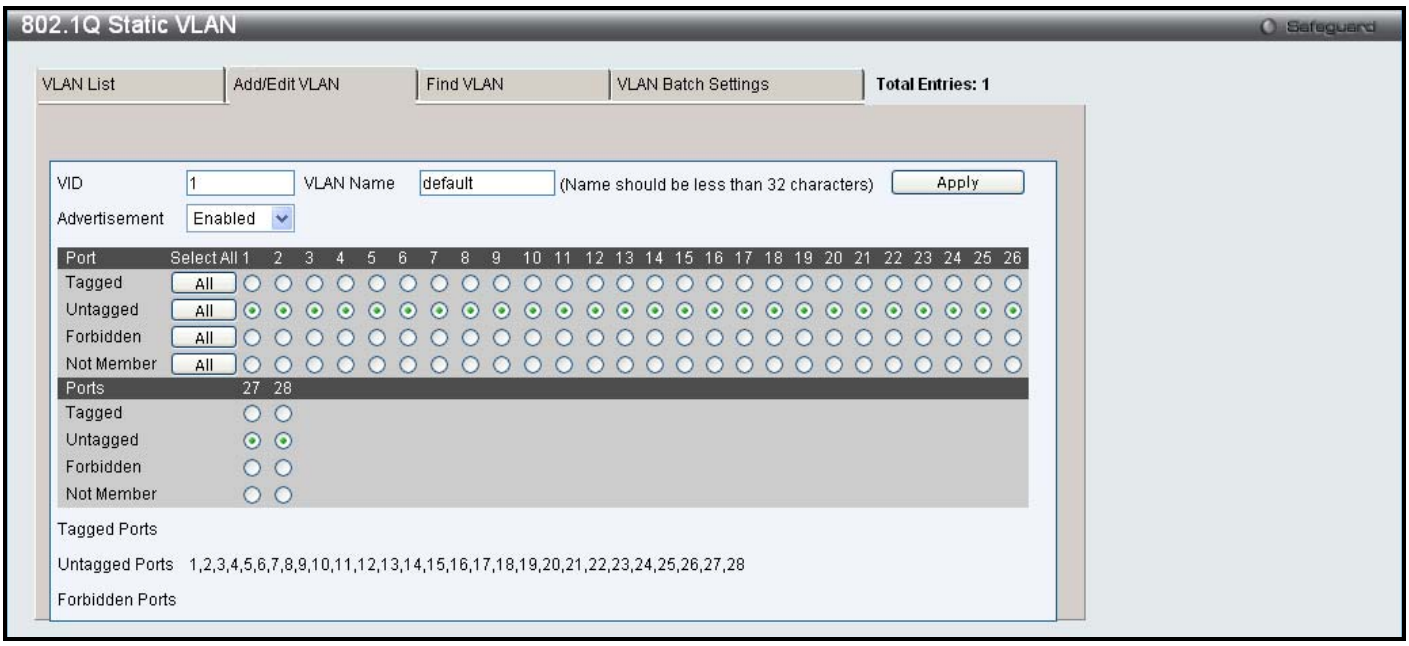


Figure 3 - 8. 802.1Q Static VLAN window – Add/Edit VLAN tab (Edit)

The following fields can then be set in the **Add/Edit VLAN** tab:

Parameter	Description
VID (VLAN ID)	Allows the entry of a VLAN ID, or displays the VLAN ID of an existing VLAN in the **Edit** window. VLANs can be identified by either the VID or the VLAN name.
VLAN Name	Allows the entry of a name for a new VLAN, or modifying the VLAN name in the **Edit** window.

	VLAN Name should be no more than 32 characters in length.
Advertisement	Enabling this function will allow the Switch to send out GVRP packets to outside sources, notifying that they may join the existing VLAN.
Port Settings	Allows an individual port to be specified as member of a VLAN.
Tagged	Specifies the port as 802.1Q tagged. Checking the box will designate the port as Tagged.
Untagged	Specifies the port as 802.1Q untagged. Checking the box will designate the port as untagged.
Forbidden	Select this to specify the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically.
Not Member	Allows an individual port to be specified as a non-VLAN member.

Click **Apply** to implement changes made.

To search for a VLAN, click the **Find VLAN** tab at the top of the window (see below), enter a VLAN ID, and click **Find** to display the settings for a previously configured VLAN.

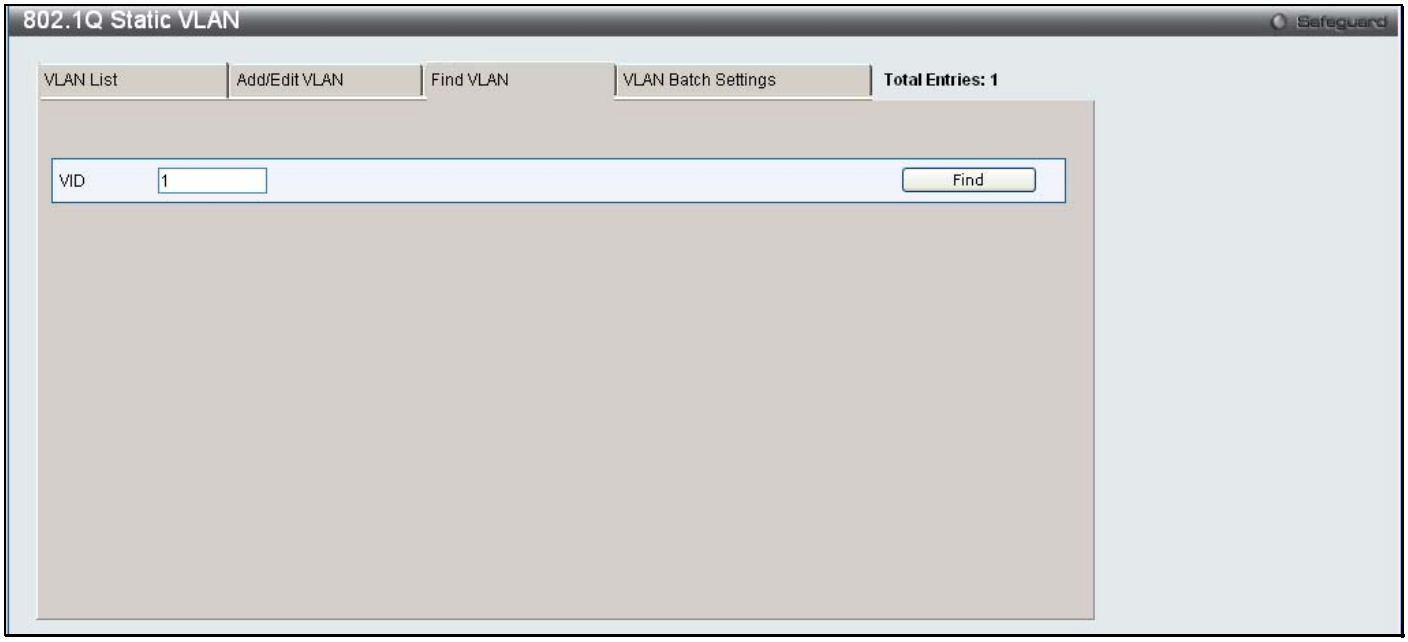


Figure 3 - 9. 802.1Q Static VLAN window – Find VLAN tab

To create a VLAN Batch entry, click the **VLAN Batch Settings** tab at the top of the window, which will display the following window:

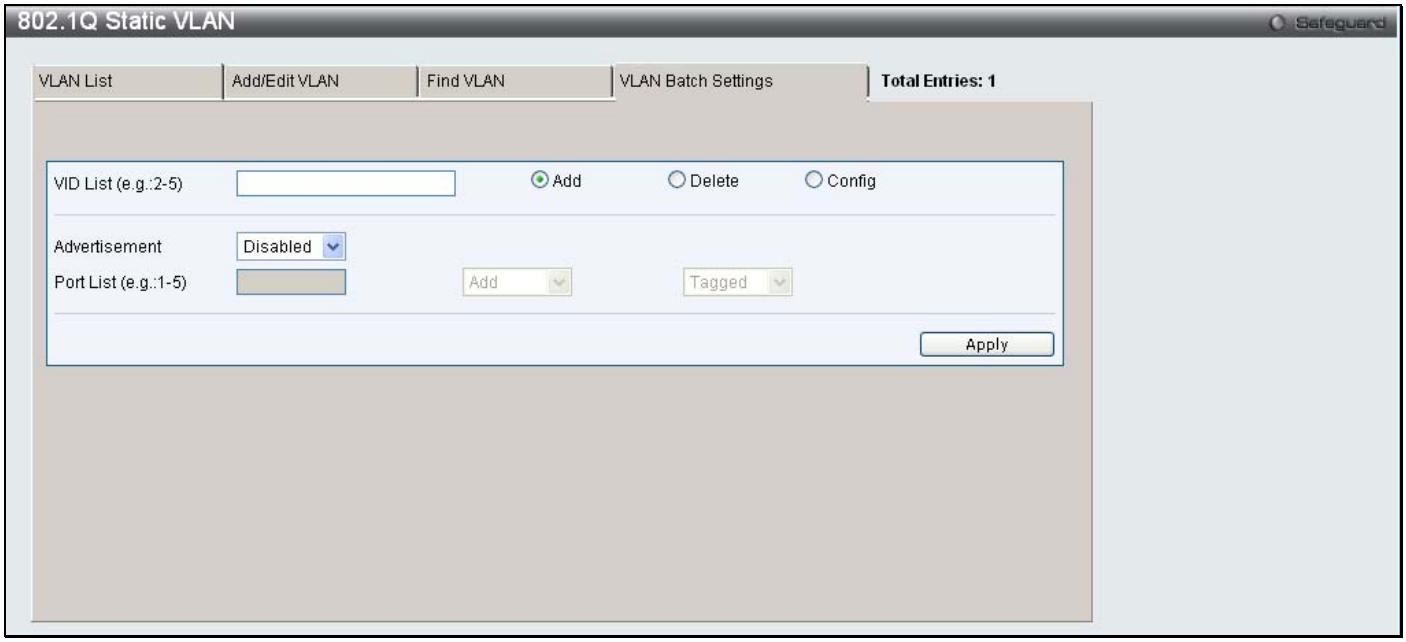


Figure 3 - 10. 802.1Q Static VLAN window – VLAN Batch Settings tab

The following fields can be set in the **VLAN Batch Settings** tab:

Parameter	Description
VID List (e.g.: 2-5)	Enter a VLAN ID List that can be added, deleted or configured.
Advertisement	Enabling this function will allow the Switch to send out GVRP packets to outside sources, notifying that they may join the existing VLAN.
Port List (e.g.: 1-5)	Allows an individual port list to be added or deleted as a member of the VLAN.
Tagged	Specifies the port as 802.1Q tagged. Checking the box will designate the port as Tagged.
Untagged	Specifies the port as 802.1Q untagged. Checking the box will designate the port as untagged.
Forbidden	Select this to specify the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically.

Click **Apply** to implement changes made.

Q-in-Q

This function allows the user to enable or disable the Q-in-Q function. Q-in-Q is designed for service providers to carry traffic from multiple users across a network.
Q-in-Q is used to maintain customer specific VLAN and Layer 2 protocol configurations even when the same VLAN ID is being used by different customers. This is achieved by inserting SPVLAN tags into the customer's frames when they enter the service provider's network, and then removing the tags when the frames leave the network.

Customers of a service provider may have different or specific requirements regarding their internal VLAN IDs and the number of VLANs that can be supported. Therefore customers in the same service provider network may have VLAN ranges that overlap, which might cause traffic to become mixed up. So assigning a unique range of VLAN IDs to each customer might cause restrictions on some of their configurations requiring intense processing of VLAN mapping tables which may exceed the VLAN mapping limit. Q-in-Q uses a single service provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer's VLAN IDs are segregated within the service provider's network even when they use the same customer specific VLAN ID. Q-in-Q expands the VLAN space available while preserving the customer's original tagged packets and adding SPVLAN tags to each new frame.

Q-in-Q Settings

To view this window, click **L2 Features > Q-in-Q > Q-in-Q Settings**:

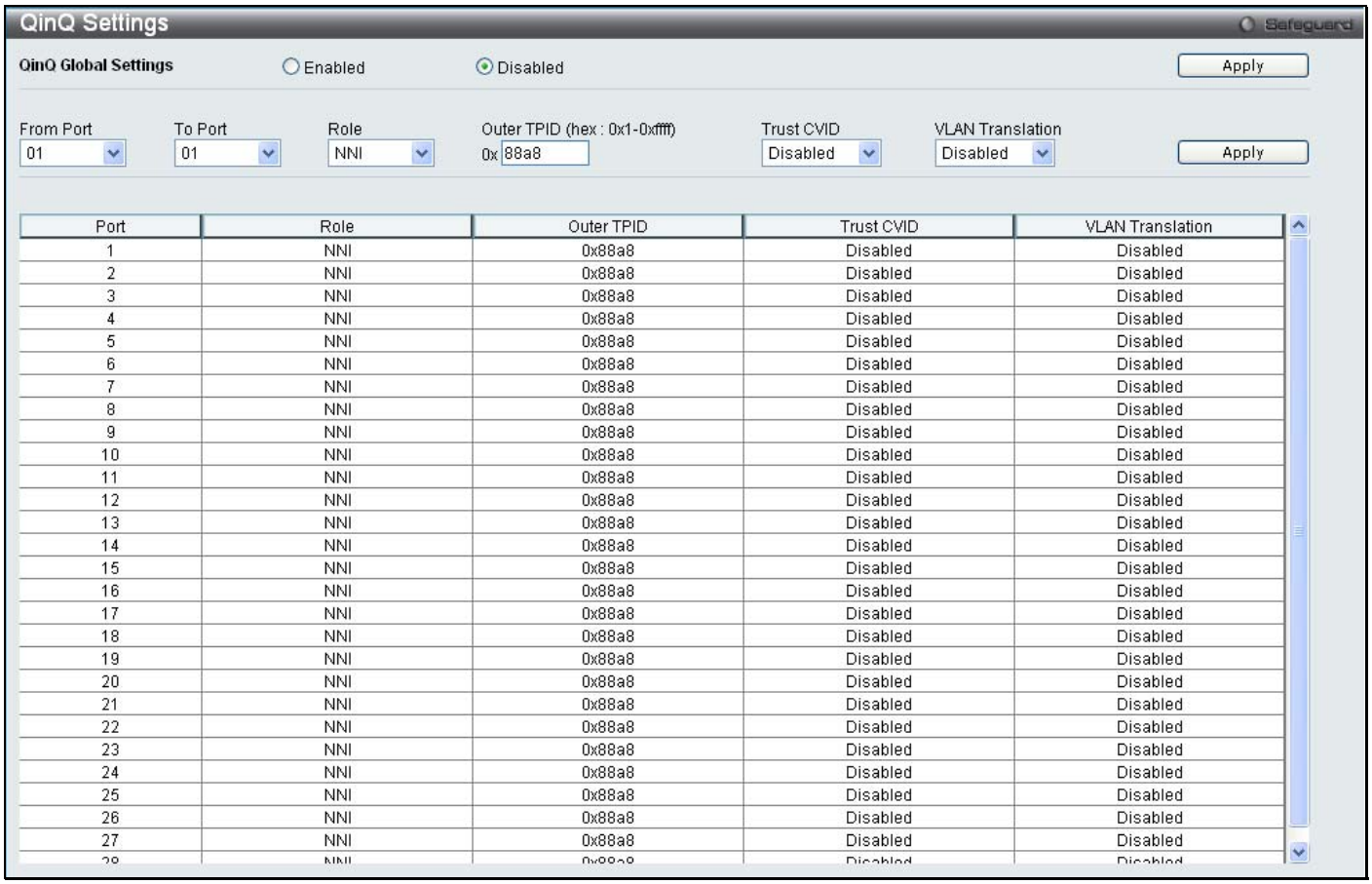


Figure 3 - 11. Q-in-Q Settings window

The following fields can be set:

Parameter	Description
Q-in-Q Global Settings	Click the radio button to enable or disable the Q-in-Q Global Settings.
From Port/To Port	A consecutive group of ports that are part of the VLAN configuration starting with the selected port.
Role	The user can choose between UNI or NNI role. *UNI* – To select a user-network interface which specifies that communication between the specified user and a specified network will occur. *NNI* – To select a network-to-network interface specifies that communication between two specified networks will occur.
Outer TPID (hex: 0x1 -0xffff)	The Outer TPID is used for learning and switching packets. The Outer TPID constructs and inserts the outer tag into the packet based on the VLAN ID and Inner Priority.
Trust CVID	Enable or disable the Trust Customer VLAN ID (CVID). If the state is *Enabled*, use the CVID from the customer's packet as the VLAN ID of the SPVLAN tag. The default is *Disabled*.
VLAN Translation	Enable or disable VLAN Translation. This translates the VLAN IDs carried in the data packets received from private networks into those used in the Service Provider's network. The default is *Disabled*. Note: To use this function, Trust CVID must also be enabled.

Click **Apply** to implement changes.

VLAN Translation Settings

VLAN translation translates the VLAN ID carried in the data packets it receives from private networks into those used in the Service Providers network.

To view this window click **L2 Features > Q-in-Q > VLAN Translation CVID Entry Settings**:

Figure 3 - 12. VLAN Translation Settings window

The following fields can be set:

Parameter	Description
Action	Specify to *Add* or *Replace* Service Provider VLAN ID (SVID) packets.
CVID (1-4094)	The customer VLAN ID List to which the tagged packets will be added.
SVID(1-4094)	This configures the VLAN to join the Service Providers VLAN as a tagged member.

Click **Apply** to make a new entry and **Delete All** to remove a VLAN Translation entry.

802.1v Protocol VLAN

The window allows the user to create Protocol VLAN groups and add protocols to that group. The 802.1v Protocol VLAN Group Settings supports multiple VLANs for each protocol and allows the user to configure the untagged ports of different protocols on the same physical port. For example it allows the user to configure an 802.1Q and 802.1v untagged port on the same physical port. The lower half of the window displays any previously created groups.

802.1v Protocol Group Settings

To view this window, click **L2 Features > 802.1v Protocol VLAN > 802.1v Protocol Group Settings**:

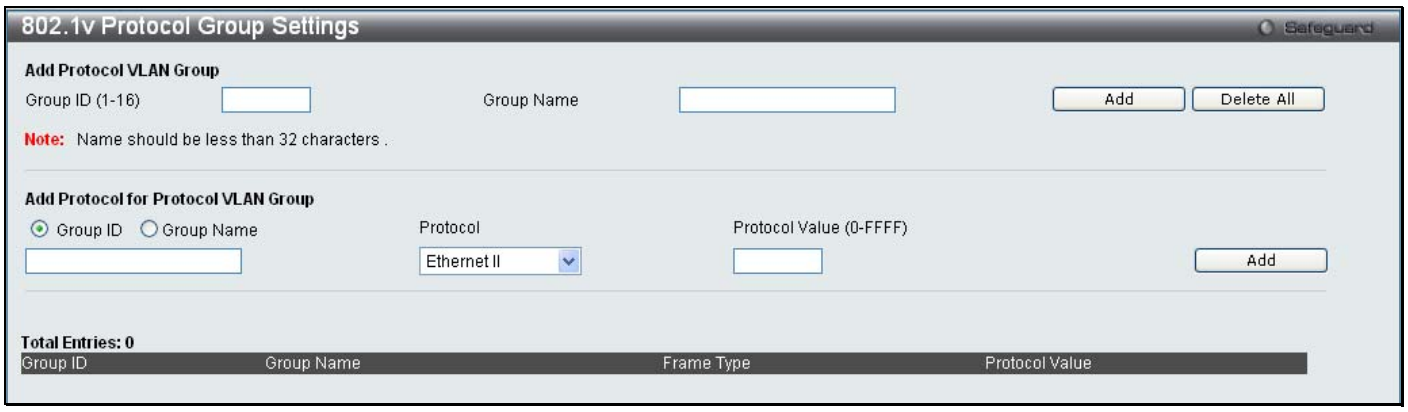


Figure 3 - 13. 802.1v Protocol Group Settings window

The following fields can be set:

Parameter	Description
Group ID (1-16)	Select an ID number for the group, between *1* and *16*.
Group Name	This is used to identify the new Protocol VLAN group. Type an alphanumeric string of up to 32 characters.
Protocol	This function maps packets to protocol-defined VLANs by examining the type octet within the packet header to discover the type of protocol associated with it. Use the drop-down menu to toggle between *Ethernet II* and *IEEE802.3 SNAP*.
Protocol Value (0-FFFF)	Enter a value for the Group.

Click **Add** to make a new entry and **Delete All** to remove an entry.

802.1v Protocol VLAN Settings

The window allows the user to configure Protocol VLAN settings. The lower half of the window displays any previously created settings.

To view this window, click **L2 Features > 802.1v Protocol VLAN > 802.1v Protocol VLAN Settings**:

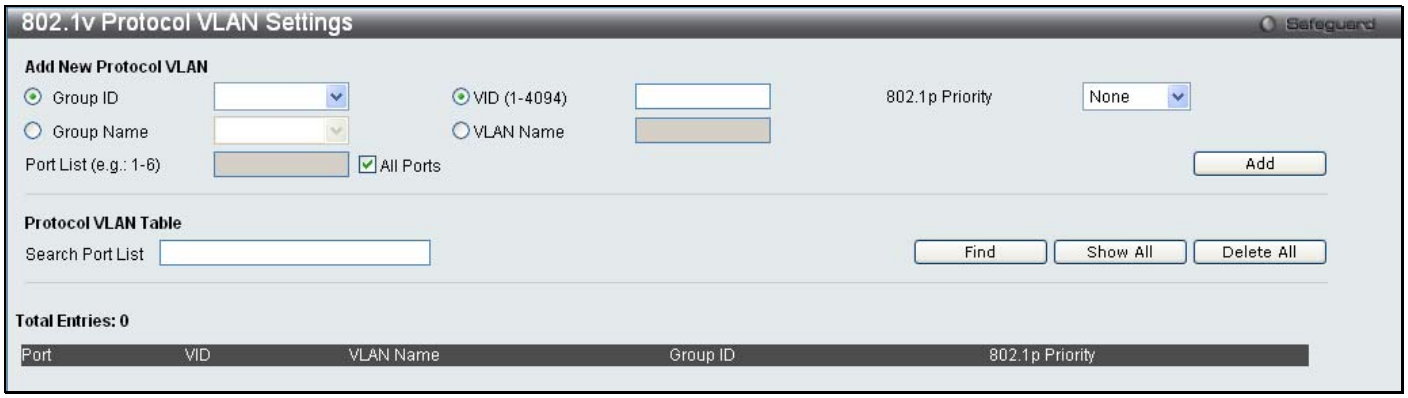


Figure 3 - 14. 802.1v Protocol VLAN Settings window

The following fields can be set:

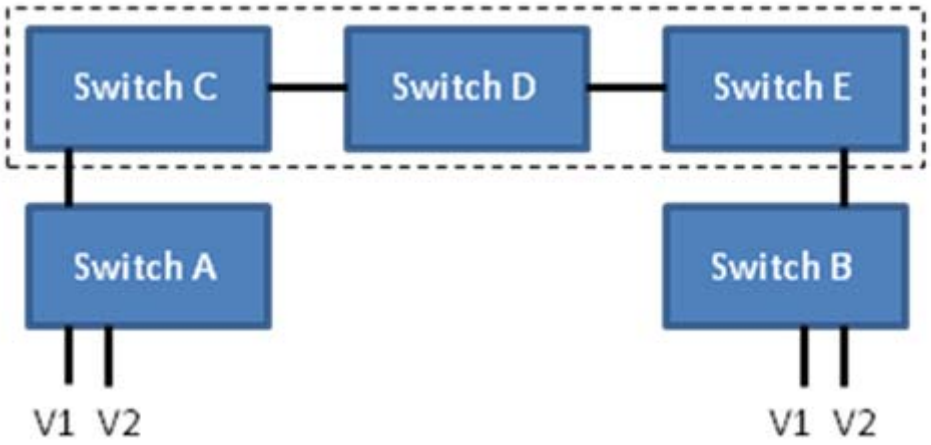
Parameter	Description
Group ID	Click the corresponding radio button to select a previously configured Group ID from the drop-down menu.
Group Name	Click the corresponding radio button to select a previously configured Group Name from the drop-down menu.
VID (1-4094)	Click the radio button to enter the VID. This is the VLAN ID that, along with the VLAN Name, identifies the VLAN the user wishes to create.
VLAN Name	Click the radio button to enter a VLAN Name. This is the VLAN Name that, along with the VLAN ID, identifies the VLAN the user wishes to create.
802.1p Priority	This parameter is specified to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.

Port List (e.g.: 1-6)	Select the specified ports you wish to configure by entering the port number in this field, or tick the Select All Ports box.
Search Port List	This function allows the user to search all previously configured port list settings and display them on the lower half of the table. To search for a port list enter the port number you wish to view and click **Find**. To display all previously configured port lists on the bottom half of the window click the **Show All** button, to clear all previously configured lists click the **Delete All** button.

VLAN Trunk Settings

Enable VLAN on a port to allow frames belonging to unknown VLAN groups to pass through that port. This is useful if you want to set up VLAN groups on end devices without having to configure the same VLAN groups on intermediary devices.

Refer to the following figure for an illustrated example. Suppose you want to create VLAN groups 1 and 2 (V1 and V2) on devices A and B. Without a VLAN Trunk, you must first configure VLAN groups 1 and 2 on all intermediary switches C, D and E; otherwise they will drop frames with unknown VLAN group tags. However, with VLAN Trunk enabled on a port(s) in each intermediary switch, you only need to create VLAN groups in the end devices (A and B). C, D and E automatically allow frames with VLAN group tags 1 and 2 (VLAN groups that are unknown to those switches) to pass through their VLAN trunking port(s).



Users can combine a number of VLAN ports together to create VLAN trunks. To create VLAN Trunk Port settings on the Switch, select the ports to be configured, change the VLAN Trunk Global State to Enabled, and click **Apply**, the new settings will appear in the VLAN Trunk Settings table in the lower part of the window.

To view the following window, click **L2 Features** > **VLAN Trunk Settings**:

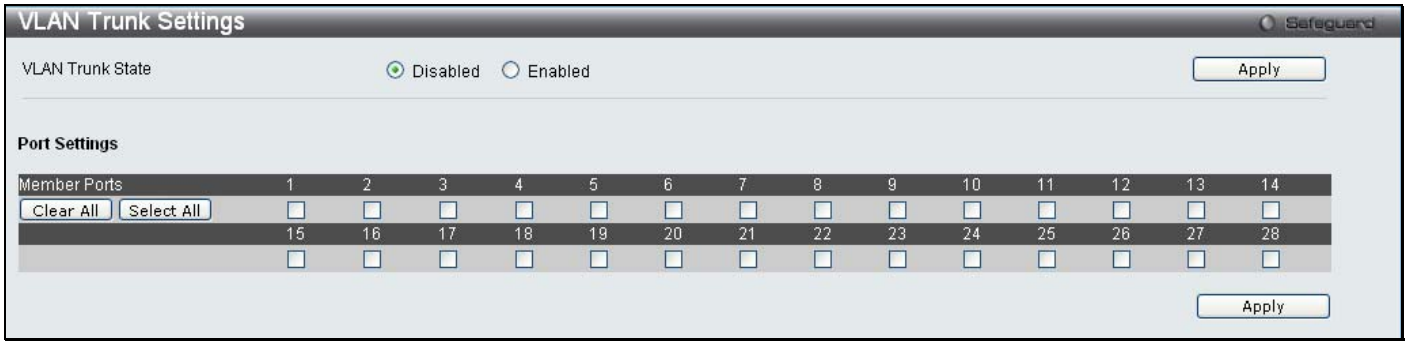


Figure 3 - 15. VLAN Trunk Settings window

The user-changeable parameters are as follows:

Parameter	Description
VLAN Trunk Global State	Enable or disable the VLAN trunking global state.
Ports	The ports to be configured.

GVRP Settings

This window allows the user to determine whether the Switch will share its VLAN configuration information with other GARP VLAN Registration Protocol (GVRP) enabled switches. In addition, Ingress Checking can be used to limit traffic by filtering incoming packets whose PVID do not match the PVID of the port. Results can be seen in the table under the configuration settings, as seen below.

To view this window, click **L2 Features > GVRP Settings**:

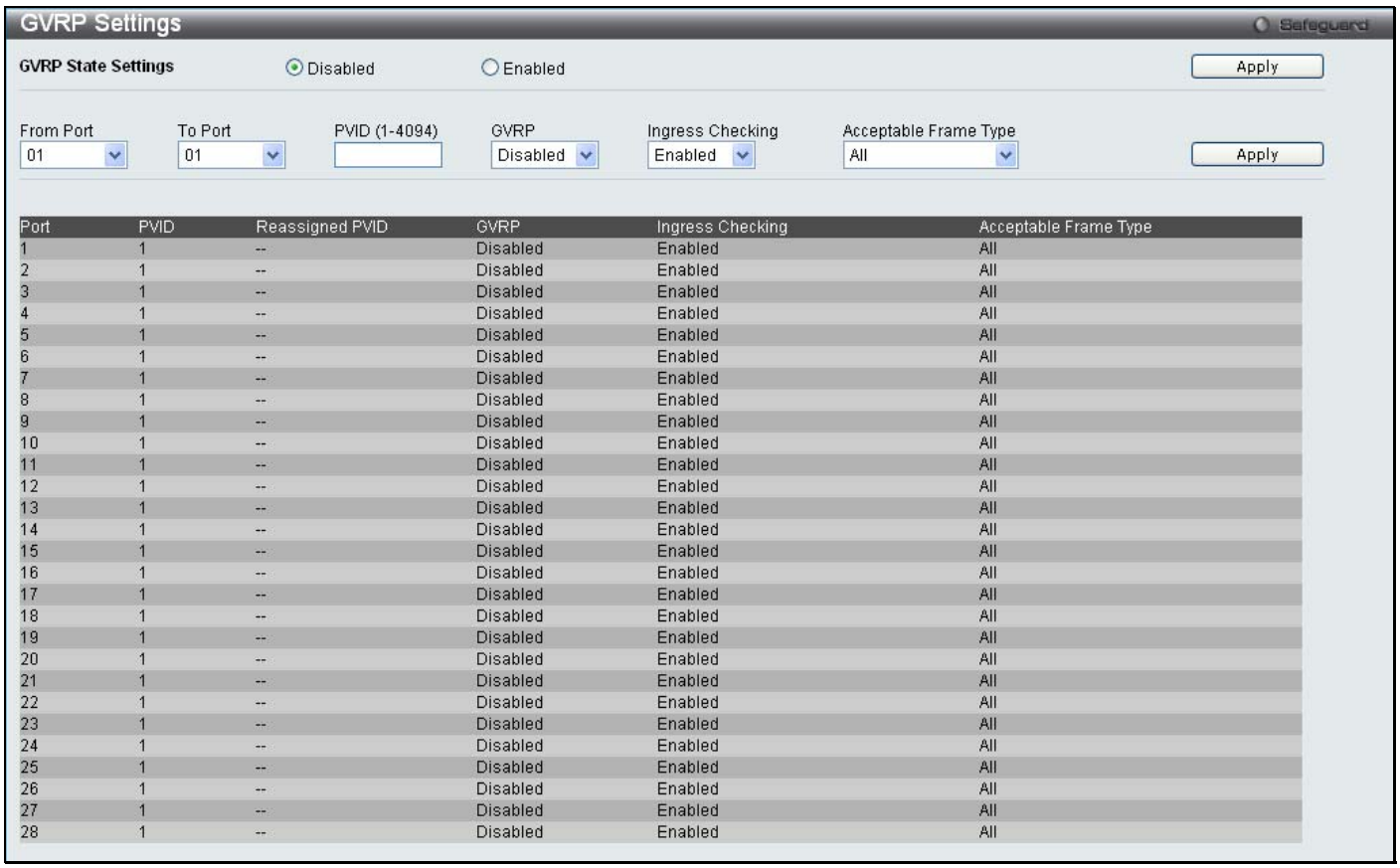

GVRP Settings
Safeguard
GVRP State Settings
Disabled
Enabled
Apply
From Port
To Port
PVID (1-4094)
GVRP
Ingress Checking
Acceptable Frame Type
01
01
Disabled
Enabled
All
Apply
Port PVID Reassigned PVID GVRP Ingress Checking Acceptable Frame Type
1 1 -- Disabled Enabled All
2 1 -- Disabled Enabled All
3 1 -- Disabled Enabled All
4 1 -- Disabled Enabled All
5 1 -- Disabled Enabled All
6 1 -- Disabled Enabled All
7 1 -- Disabled Enabled All
8 1 -- Disabled Enabled All
9 1 -- Disabled Enabled All
10 1 -- Disabled Enabled All
11 1 -- Disabled Enabled All
12 1 -- Disabled Enabled All
13 1 -- Disabled Enabled All
14 1 -- Disabled Enabled All
15 1 -- Disabled Enabled All
16 1 -- Disabled Enabled All
17 1 -- Disabled Enabled All
18 1 -- Disabled Enabled All
19 1 -- Disabled Enabled All
20 1 -- Disabled Enabled All
21 1 -- Disabled Enabled All
22 1 -- Disabled Enabled All
23 1 -- Disabled Enabled All
24 1 -- Disabled Enabled All
25 1 -- Disabled Enabled All
26 1 -- Disabled Enabled All
27 1 -- Disabled Enabled All
28 1 -- Disabled Enabled All

Figure 3 - 16. GVRP Settings window

The following fields can be set:

Parameter	Description
GVRP State Settings	Click the radio buttons to enable or disable the GVRP global state settings.
From Port/To Port	These two fields allow you to specify the range of ports that will be included in the Port-based VLAN that you are creating using the **802.1Q Port Settings** window.
PVID (1-4094)	Enter a PVID assignment for each port, which may be manually assigned to a VLAN when created in the 802.1Q Port Settings table. The Switch's default is to assign all ports to the default VLAN with a VID of 1. The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified to accept only tagged frames - as tagging, and an untagged packet is forwarded to the port for transmission, the port will add an 802.1Q tag using the PVID to write the VID in the tag. When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions. If the port receives a packet, and Ingress filtering is enabled, the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet.
GVRP	The Group VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN. GVRP is *Disabled* by default.
Ingress Checking	This field can be toggled using the space bar between *Enabled* and *Disabled*. *Enabled* enables

	the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet. *Disabled* disables ingress filtering. Ingress Checking is *Enabled* by default.
Acceptable Frame Type	This field denotes the type of frame that will be accepted by the port. The user may choose between *Tagged Only*, which means only VLAN tagged frames will be accepted, and *All*, which mean both tagged and untagged frames will be accepted. *All* is enabled by default.

Click **Apply** to implement changes made.

Asymmetric VLAN Settings

Shared VLAN Learning is a primary example of the requirement for Asymmetric VLANs. Under normal circumstances, a pair of devices communicating in a VLAN environment will both send and receive using the same VLAN; however, there are some circumstances in which it is convenient to make use of two distinct VLANs, one used for A to transmit to B and the other used for B to transmit to A in these cases Asymmetric VLANs are needed. An example of when this type of configuration might be required would be if the client was on a distinct IP subnet, or if there was some confidentiality-related need to segregate traffic between the clients.

To view this window, click **L2 Features > Asymmetric VLAN Settings**:

Figure 3 - 17. Asymmetric VLAN Settings window

Click **Apply** to implement changes.

MAC-based VLAN Settings

This window is used to create MAC-based VLAN entries on the switch. A MAC Address can be mapped to any existing static VLAN and multiple MAC addresses can be mapped to the same VLAN. When a static MAC-based VLAN entry is created for a user, the traffic from this user is able to be serviced under the specified VLAN. Therefore each entry specifies a relationship of a source MAC address with a VLAN.

To view this window, click **L2 Features > MAC-based VLAN Settings**:

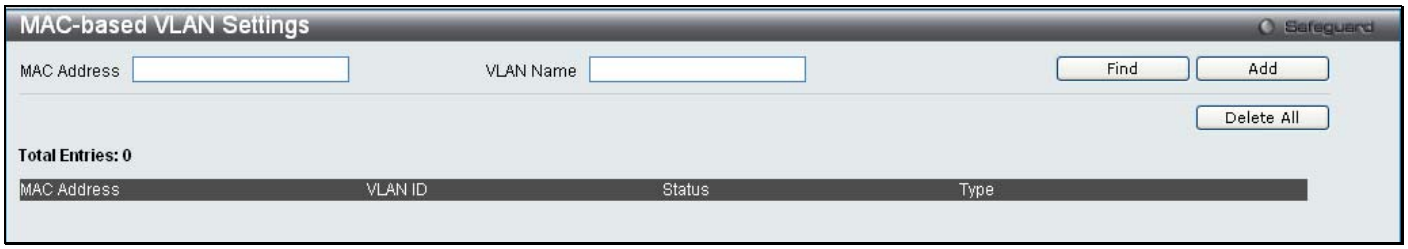


Figure 3 - 18. MAC-based VLAN Settings window

The following fields can be set

Parameter	Description
MAC Address	Specify the MAC address to be mapped.
VLAN Name	Enter the VLAN name of a previously configured VLAN.

Click **Find**, **Add** or **Delete All** for changes to take affect.

PVID Auto Assign Settings

This enables or disables PVID Auto Assign on the Switch. PVID is the VLAN that the switch will use for forwarding and filtering purposes. If PVID Auto-Assign is *Enabled*, PVID will be possibly changed by previously set PVID or VLAN configurations. When a user configures a port to VLAN X's untagged membership, this port's PVID will be updated with VLAN X. In the form of a VLAN list command, PVID is updated with the last item on the VLAN list. When a user removes a port from the untagged membership of the PVID's VLAN, the port's PVID will be assigned to a default VLAN. When PVID Auto Assign is *Disabled*, PVID can only be changed by PVID configuration (user changes explicitly). The VLAN configuration will not automatically change the PVID. The default setting is *Enabled*.

To view this window, click **L2 Features > PVID Auto Assign Settings**:

Figure 3 - 19. PVID Auto Assign Settings window

Port Trunking

Understanding Port Trunk Groups

Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline. The Switch supports up to fourteen port trunk groups with two to eight ports in each group.

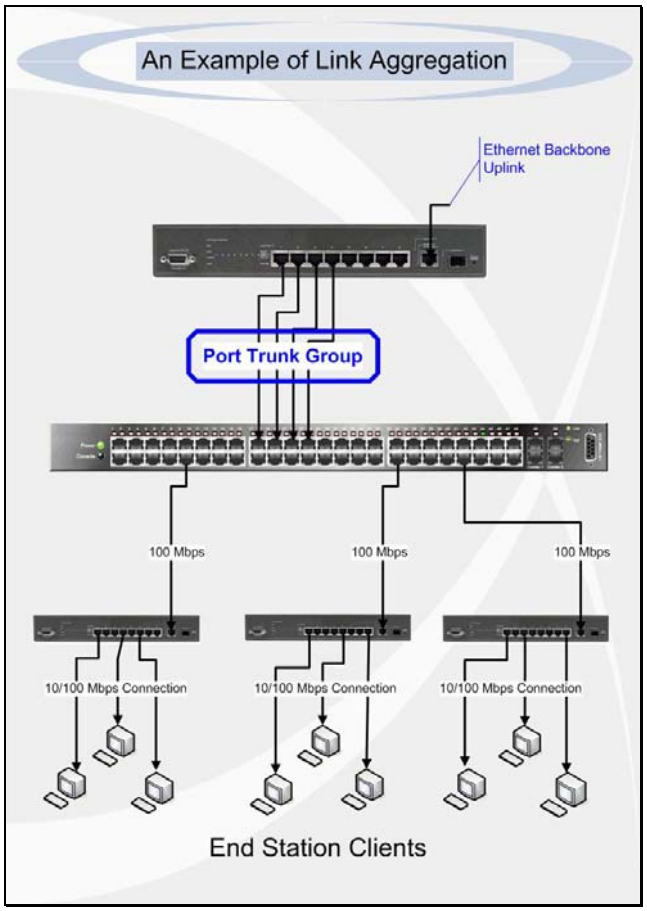


Figure 3 - 20 Example of Port Trunk Group

The Switch treats all ports in a trunk group as a single port. Data transmitted to a specific host (destination address) will always be transmitted over the same port in a trunk group. This allows packets in a data stream to arrive in the same order they were sent.

NOTE: If any ports within the trunk group become disconnected, packets intended for the disconnected port will be load shared among the other unlinked ports of the link aggregation group.

Link aggregation allows several ports to be grouped together and to act as a single link. This gives a bandwidth that is a multiple of a single link's bandwidth.

Link aggregation is most commonly used to link a bandwidth intensive network device or devices, such as a server, to the backbone of a network.

The Switch allows the creation of up to fourteen link aggregation groups, each group consisting of two to eight links (ports). All of the ports in the group must be members of the same VLAN, and their STP status, static multicast, traffic control; traffic segmentation and 802.1p default priority configurations must be identical. Port locking, port mirroring and 802.1X must not be enabled on the trunk group. Further, the aggregated links must all be of the same speed and should be configured as full duplex.

The Master Port of the group is to be configured by the user, and all configuration options, including the VLAN configuration that can be applied to the Master Port, are applied to the entire link aggregation group.

Load balancing is automatically applied to the ports in the aggregated group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

The Spanning Tree Protocol will treat a link aggregation group as a single link, on the switch level. On the port level, the STP will use the port parameters of the Master Port in the calculation of port cost and in determining the state of the link aggregation group. If two redundant link aggregation groups are configured on the Switch, STP will block one entire group; in the same way STP will block a single port that has a redundant link.

To view this window, click **L2 Features > Port Trunking**:

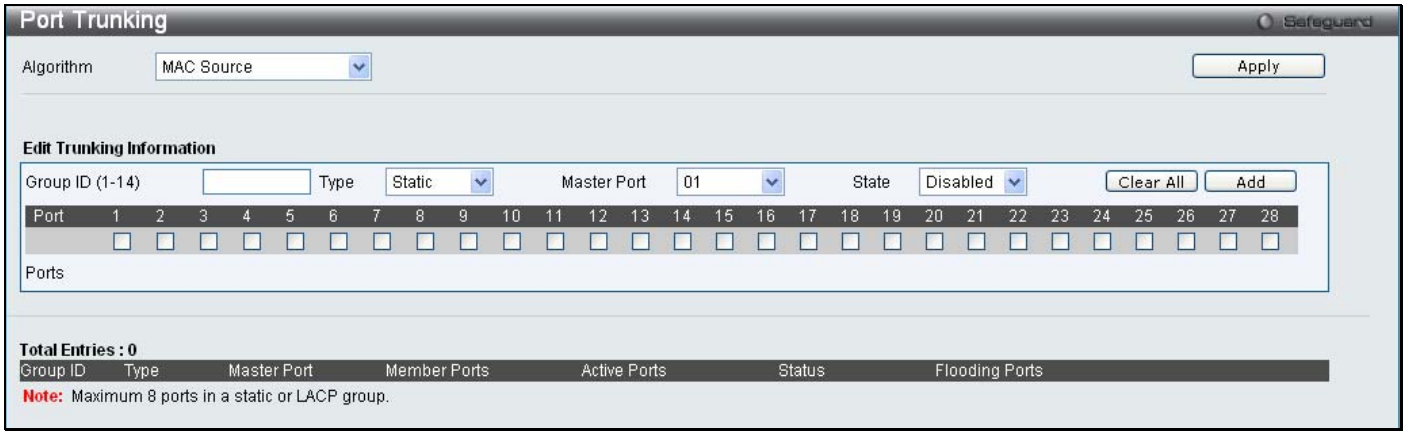


Figure 3 - 21. Port Trunking window

The following fields can be set

Parameter	Description
Algorithm	The algorithm that the Switch uses to balance the load across the ports that make up the port trunk group is defined by this definition. Choose *MAC Source*, *MAC Destination*, *MAC Source Dest*, *IP Source, IP Destination* or *IP Source Dest* (See the Link Aggregation section of this manual).
Group ID (1-14)	Select an ID number for the group, between *1* and *14*.
Type	This pull-down menu allows you to select between *Static* and *LACP* (Link Aggregation Control Protocol). *LACP* allows for the automatic detection of links in a Port Trunking Group.
Master Port	Choose the Master Port for the trunk group using the pull-down menu.
State	Trunk groups can be toggled between *Enabled* and *Disabled*. This is used to turn a port trunking group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device or to have an absolute backup aggregation group that is not under automatic control.
Active Ports	Shows the ports that are currently forwarding packets.

(Member) Ports	Choose the members of a trunked group. Up to eight ports per group can be assigned to a group.
Flooding Ports	These ports are designated for flooding broadcast, multicast, and DLF (unicast Destination Lookup Fail) packets from the CPU in a trunk group. The port is defined by software and doesn't actually exist in the hardware.

Click **Apply** to implement changes made.

LACP Port Settings

This window is used to create port trunking groups on the Switch. The user may set which ports will be active and passive in processing and sending LACP control frames.

To view this window, click **L2 Features > LACP Port Settings**:

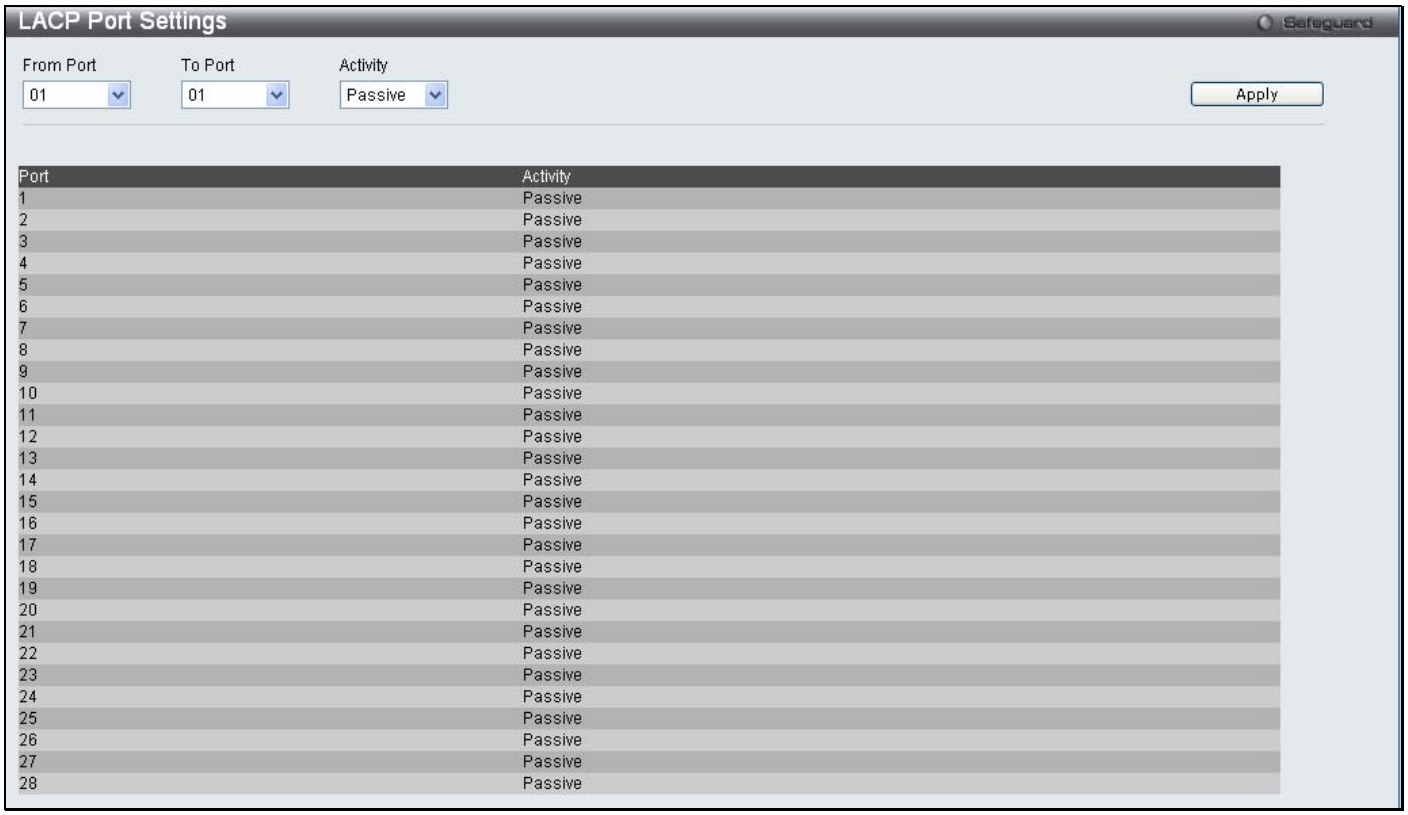


Figure 3 - 22. LACP Port Settings window

The following fields can be set

Parameter	Description
From Port/To Port	A consecutive group of ports may be configured starting with the selected port.
Activity	*Active* - Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP. *Passive* - LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, one end of the connection must have "active" LACP ports (see above).

Click **Apply** to implement changes made.

Traffic Segmentation

Traffic segmentation is used to limit traffic flow from a single port to a group of ports on the Switch. This method of segmenting the flow of traffic is similar to using VLANs to limit traffic, but is more restrictive. It provides a method of directing traffic that does not increase the overhead of the Switch CPU. This window allows the user to view which ports on the Switch are allowed to forward packets to other ports on the Switch. To configure new forwarding ports for a particular port, select a port from the From Port and To Port drop-down menus and click **Apply**.

To view this window, click **L2 Features > Traffic Segmentation**:

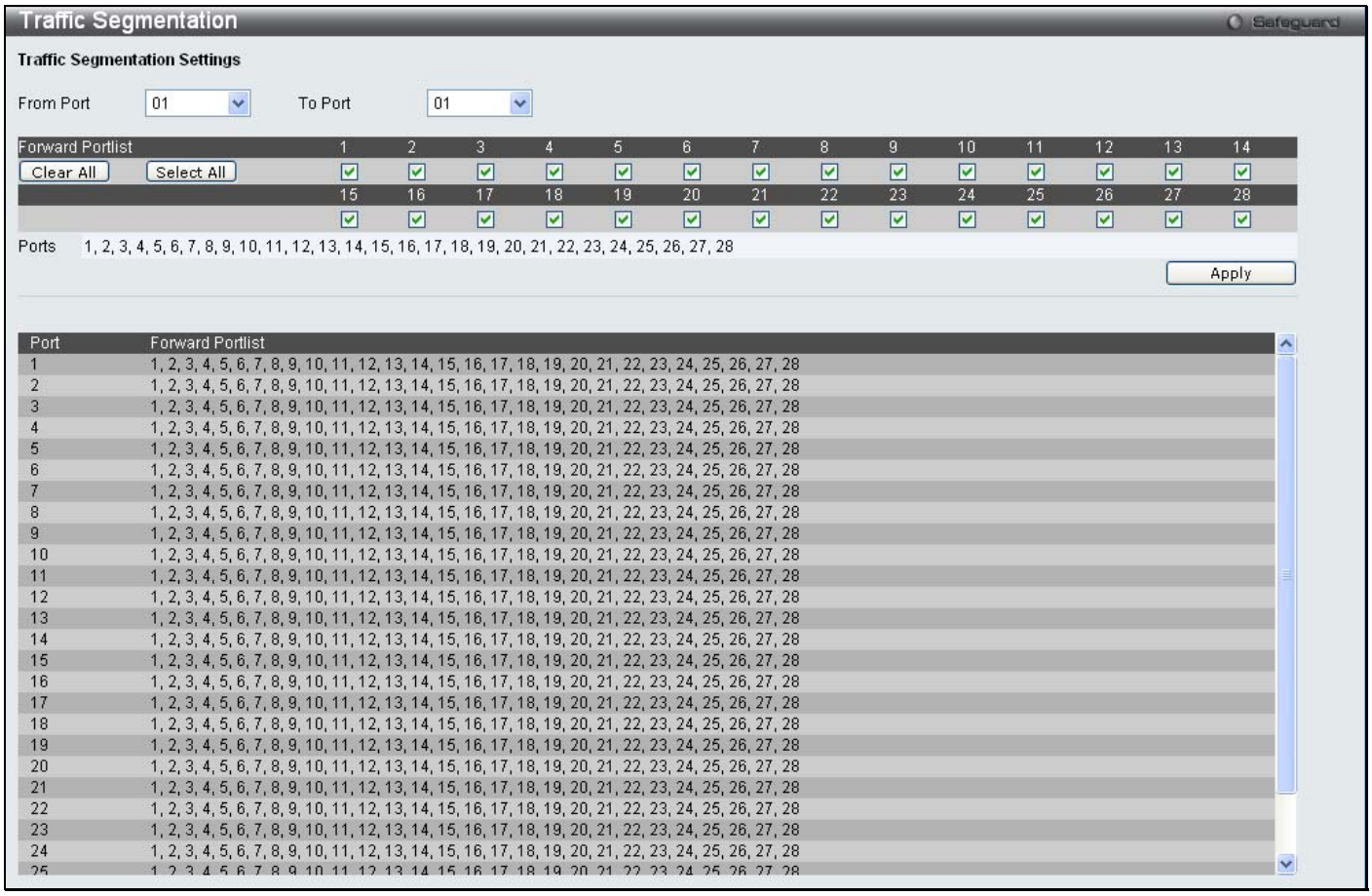

Traffic Segmentation
Safeguard
Traffic Segmentation Settings
From Port
01
To Port
01
Forward Portlist
1 2 3 4 5 6 7 8 9 10 11 12 13 14
Clear All
Select All
15 16 17 18 19 20 21 22 23 24 25 26 27 28
Ports
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28
Apply
Port
Forward Portlist

Figure 3 - 23. Traffic Segmentation window

The following fields can be set

Parameter	Description
From Port/To Port	Check the corresponding boxes for the port(s) to transmit packets.
Forward Portlist	Check the boxes to select which of the ports on the Switch will be able to forward packets. These ports will be allowed to receive packets from the port specified above.

Clicking the **Apply** button will enter the combination of transmitting port and allowed receiving ports into the Switch's Current Traffic Segmentation Table.

BPDU Tunneling Settings

To view this window, click **L2 Features > BPDU Tunneling Settings**:

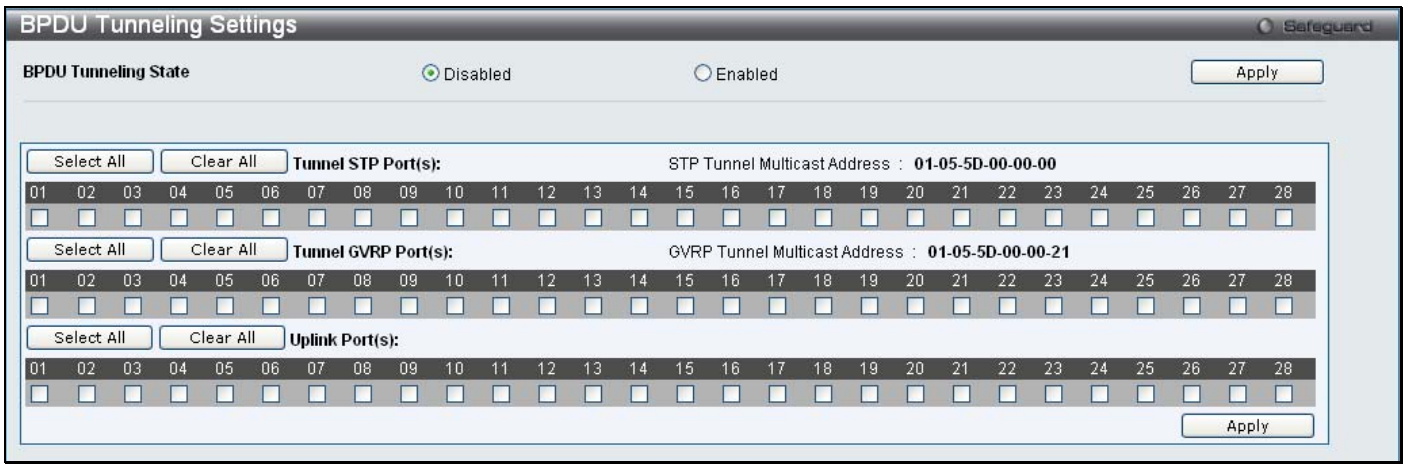


Figure 3 - 24. BPDU Tunneling Settings window

IGMP Snooping

Internet Group Management Protocol (IGMP) snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host. When enabled for IGMP snooping, the Switch can add or remove a port to a specific device based on IGMP messages passing through the Switch.

In order to use IGMP Snooping, it must first be enabled for the entire Switch. Then, fine-tune the settings for each VLAN using the **IGMP Snooping** windows in the **L2 Features** folder. When enabled for IGMP snooping, the Switch can open or close a port to a specific multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa. The Switch monitors IGMP messages and discontinues forwarding multicast packets when there are no longer hosts requesting that they continue.

IGMP Snooping Settings

Use this window to enable or disable IGMP snooping on the Switch. The IGMP Snooping State under IGMP Snooping Global Settings can be enabled or disabled and a Max Learning Entry Value between 1 and 1024 can be entered in the field under IGMP Data Driven Learning Settings. Click **Apply** to modify the settings.

To view this window, click **L2 Features > IGMP Snooping > IGMP Snooping Settings**:

Figure 3 - 25. IGMP Snooping Settings window

Clicking the **Edit** button will open this window:

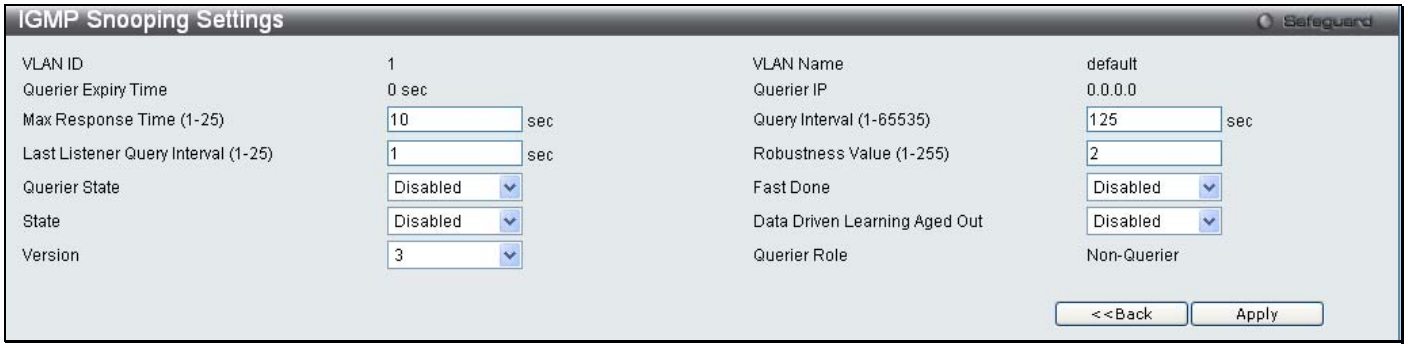


Figure 3 - 26. IGMP Snooping Settings (Edit) window

The following fields can be set.

Parameter	Description
VLAN ID	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN for which the user wishes to modify the IGMP Snooping Settings.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN for which the user wishes to modify the IGMP Snooping Settings.
Querier Expiry Time	Displays the querier expiry time.
Querier IP	The IP address of the device which acts as the IGMP querier for the network.
Max Response Time (1-25)	This determines the maximum amount of time in seconds to wait for reports from members. The Max Response Time field allows an entry between *1* and *25* (seconds). The default is *10*.
Query Interval (1-65535)	The Query Interval field is used to set the time (in seconds) between transmitting IGMP queries. Entries between *1* and *65535* seconds are allowed. The default is *125*.
Last Listener Query Interval (1-25)	This field specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. The default is *1*.
Robustness Value (1-255)	Adjust this variable according to expected packet loss. If packet loss on the VLAN is expected to be high, the Robustness Variable should be increased to accommodate increased packet loss. This entry field allows an entry of *1* to *255*. The default is *2*.
Querier State	Choose *Enabled* to enable transmitting IGMP query packets or *Disabled* to disable the transmitting of IGMP query packets. The default is *Disabled*.
Fast Done	This parameter allows the user to enable the Fast Leave function. Enabled, this function will allow members of a multicast group to leave the group immediately (without the implementation of the Last Member Query Timer) when an IGMP Leave Report Packet is received by the Switch. The default is *Disabled*.
State	Select *Enabled* to implement IGMP Snooping. This field is *Disabled* by default.
Data Driven Learning Aged Out	Allows users to enable or disable aged out of IGMP Snooping data driven learning for the specified VLAN.
Version	Allows the user to configure the IGMP version used on the Switch. The default value is *3*.
Querier Role	This read-only field describes the behavior of the Switch for sending query packets. Querier will denote that the Switch is sending out IGMP query packets. Non-Querier will denote that the Switch is not sending out IGMP query packets. This field will only read Querier when the Querier State and the State fields have been *Enabled*.

To modify the IGMP Snooping Router Port Settings, click on the Modify Router Port hyperlink, which will show the following window for the user to configure:

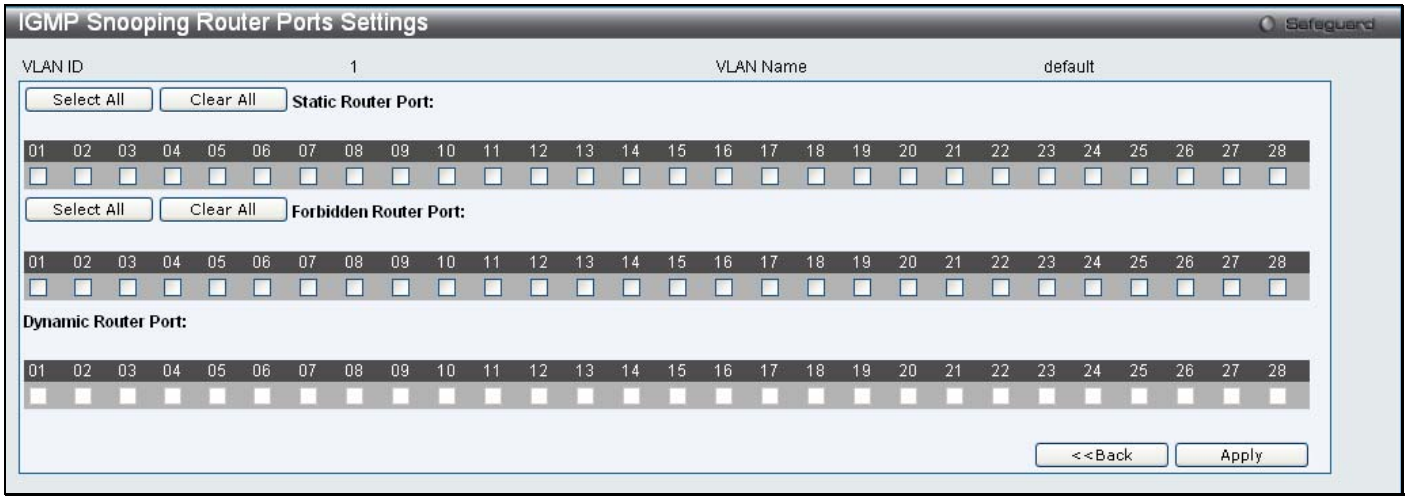


Figure 3 - 27. IGMP Snooping Router Ports Settings window

Select the desired member ports and click **Apply**. Click **<<Back** to go back to the **IGMP Snooping Settings** window.

IGMP Access Control Settings

This window is used to configure IGMP Access Control settings on the Switch.

To view this window, click **L2 Features > IGMP Snooping > IGMP Access Control Settings**:

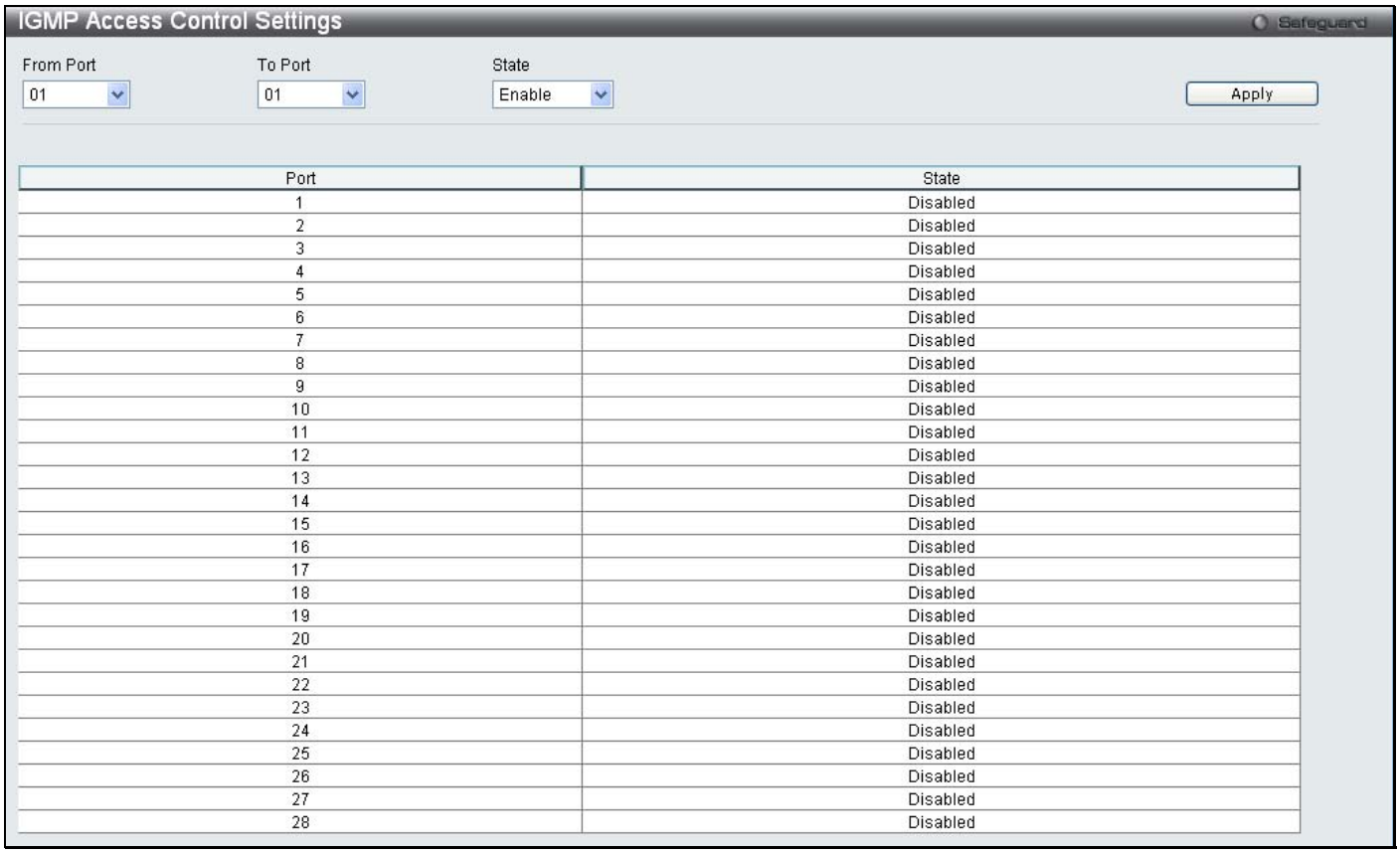


Figure 3 - 28. IGMP Access Control Settings window

Parameter	Description
From Port/To Port	Select a range of ports.
State	Enable or disable the IGMP Access Control. When *Enable* is selected and the Switch receives an IGMP Join request, the Switch will send the access request to the RADIUS server to do the authentication.

Click **Apply** to implement changes made.

IGMP Snooping Multicast VLAN Settings

This window is used to configure the IGMP Snooping Multicast VLAN settings on the Switch.

To view this window, click **L2 Features > IGMP Snooping > IGMP Snooping Multicast VLAN Settings**:

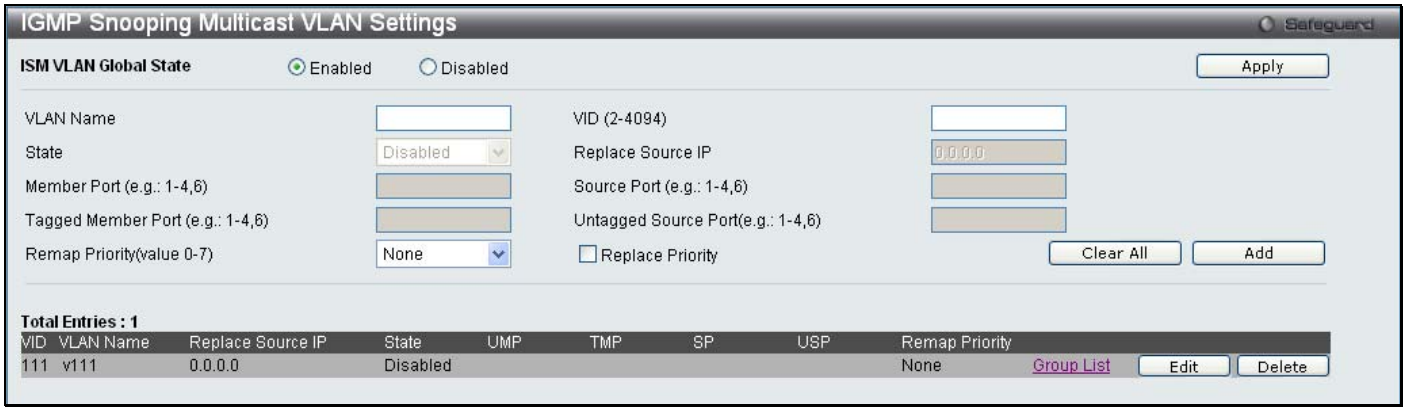


Figure 3 - 29. IGMP Snooping Multicast VLAN Settings window

The following fields can be set

Parameter	Description
ISM VLAN Global State	Click the Enabled or Disabled radio button to enable or disable multicast VLAN.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN the user wishes to add or modify the IGMP Snooping Settings for.
VID (2-4094)	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN the user wishes to add or modify the IGMP Snooping Settings for.
State	Enable or disable multicast VLANs for the chosen VLAN.
Replace Source IP	With the IGMP snooping function, the IGMP report packet sent by the host will be forwarded to the source port. Before forwarding of the packet, the source IP address in the join packet needs to be replaced by this IP address. If none is specified, the source IP address will not be replaced.
Member Port (e.g.: 1-4, 6)	A range of member ports to add to the multicast VLAN. They will become the untagged member ports of the ISM VLAN.
Source Port (e.g.: 1-4, 6)	Select the source Port for the multicast VLAN.
Tagged Member Port (e.g.: 1-4, 6)	Specifies the ports that will be tagged as members of the multicast VLAN.
Untagged Source Port (e.g.: 1-4, 6)	A range of untagged source ports to add to the multicast VLAN. The reassigned PVID of the untagged source port will be automatically changed to the multicast VLAN.
Remap Priority (Value 0-7)	The remap priority is associated with the data traffic to be forwarded on the multicast VLAN. If *None* is selected, the packet's original priority will be used.The default setting is *None*.
Replace Priority	Tick this option so that the packet's priority will be changed based on the remap priority by the Switch. This option takes effect only when remap priority is set.

To edit an entry, click the corresponding **Edit** button. To delete an entry, click the corresponding **Delete** button.

To add a multicast VLAN to a profile that has been created, click the corresponding hyperlinked Group List to reveal the following window:

Figure 3 - 30. IGMP Snooping Multicast VLAN Group List Settings window

Enter a Multicast Address and click **Add**. The new information will be displayed in the table at the bottom of the window. Click Show IGMP Snooping Multicast VLAN Entries to return to the **IGMP Snooping Multicast VLAN Settings** window. Click **Delete All** to remove all the entries on this window.

IP Multicast Profile Settings

This window allows the user to add a profile to which multicast IP address reports are to be received on specified ports on the Switch. This function will therefore limit the number of reports received and the number of multicast groups configured on the Switch. The user may set an IP Multicast address or range of IP Multicast addresses to accept reports (Permit) or deny reports (Deny) coming into the specified switch ports.

To view this window, click **L2 Features > IGMP Snooping > IP Multicast Profile Settings**:

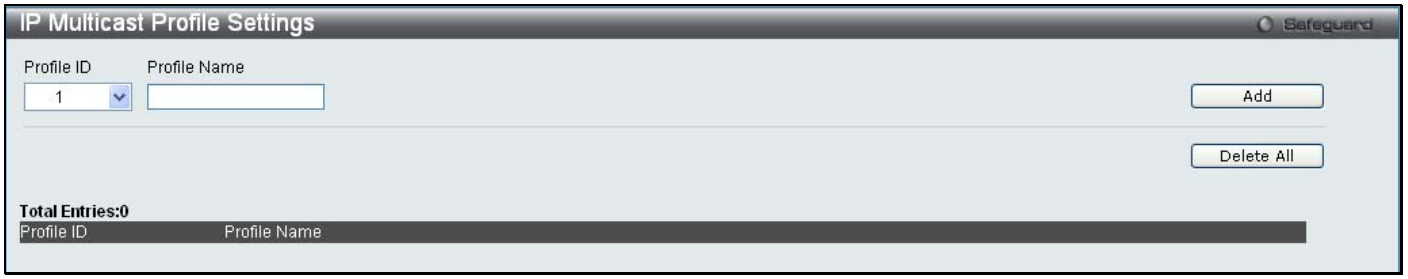


Figure 3 - 31. IP Multicast Profile Settings window

The following fields can be set

Parameter	Description
Profile ID	Use the drop-down menu to choose a Profile ID.
Profile Name	Enter a name for the IP Multicast Profile.

To edit and entry click the corresponding **Edit** button and to delete an entry click the corresponding **Delete** button.

Figure 3 - 32. IP Multicast Profile Settings (Edit) window

To configure the Group List Settings click the hyperlinked Group List. The following window will appear:

Figure 3 - 33. Multicast Address Group List Settings window

Enter the Multicast Address List starting with the lowest in the range, and click **Add**. To return to the **IP Multicast Profile Settings** window, click the **<<Back** button.

Limited Multicast Range Settings

This window enables the user to configure the ports on the Switch that will be involved in the Limited IP Multicast Range. The user can configure the range of ports and associate an IP Multicast Profile to allow or disallow IGMP join requests to multicast groups defined in the profile.

To configure these settings, click **L2 Features > IGMP Snooping > Limited Multicast Range Settings**:

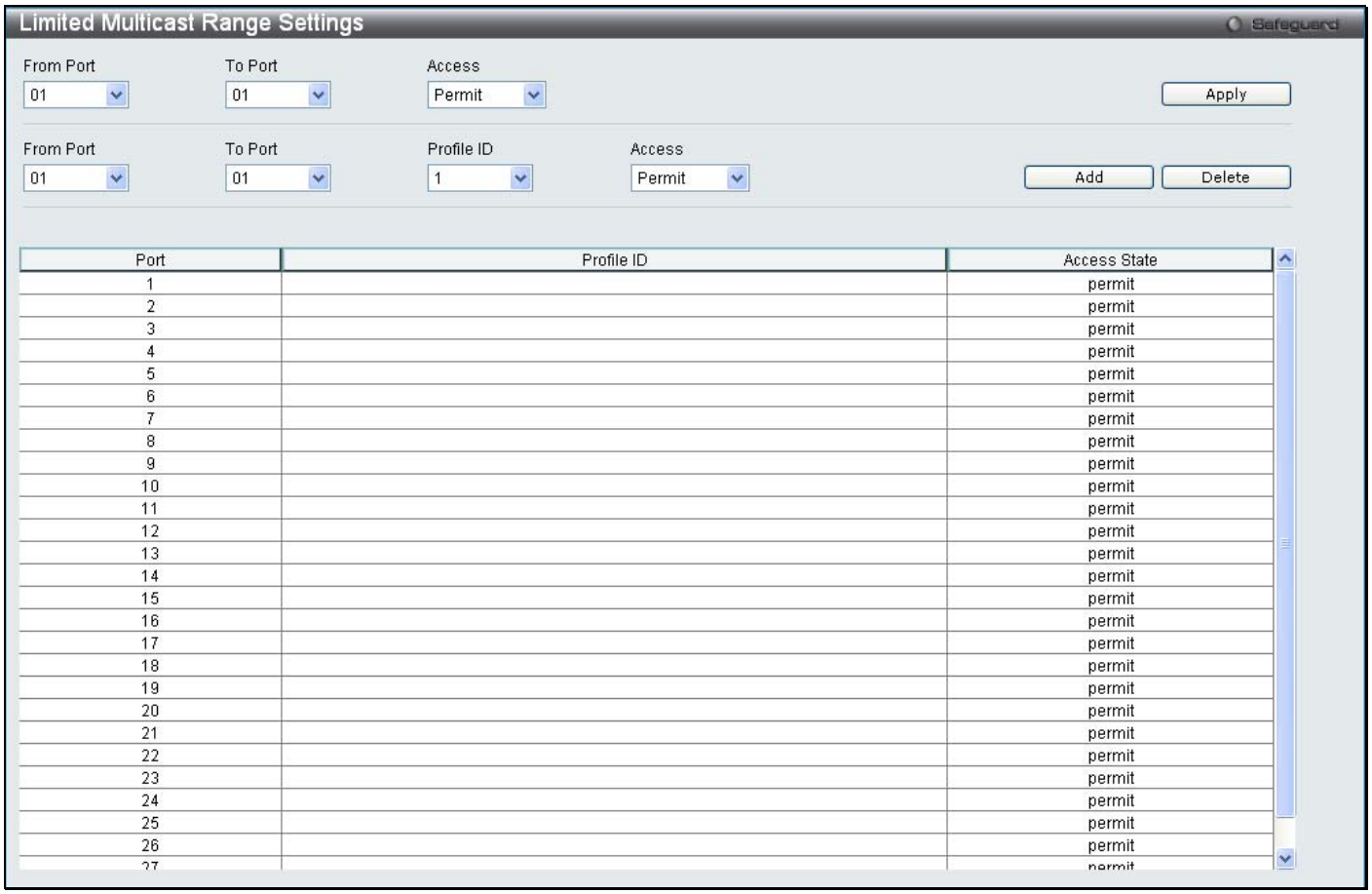


Figure 3 - 34. Limited Multicast Range Settings window

To add a new range enter the information and click **Add**, to delete an entry enter the information and click **Delete**.

Max Multicast Group Settings

This window allows users to configure the ports on the Switch that will be a part of the maximum number of multicast groups that can be learned. To add a new Max Multicast Group, enter the information and click **Apply**.

To view this window, click **L2 Features > IGMP Snooping > Max Multicast Group Settings**:

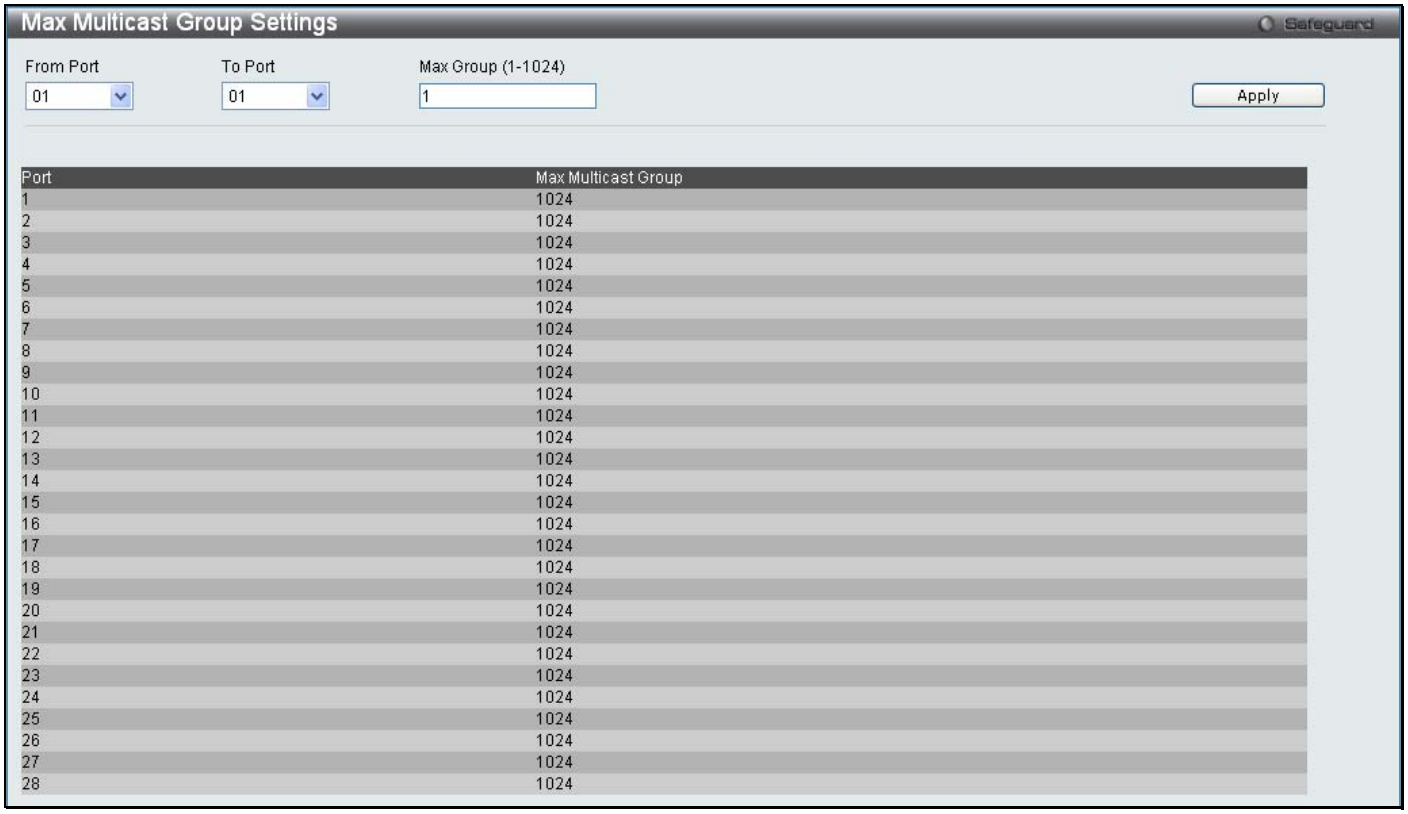


Figure 3 - 35. Max Multicast Group Settings window

The following fields can be set:

Parameter	Description
From Port/To Port	Use the drop-down menus to choose a range of ports.
Max Group (1-1024)	Enter the maximum number of the multicast groups. The range is from *1* to *1024*.

MLD Snooping Settings

Multicast Listener Discovery (MLD) Snooping is an IPv6 function used similarly to IGMP snooping in IPv4. It is used to discover ports on a VLAN that are requesting multicast data. Instead of flooding all ports on a selected VLAN with multicast traffic, MLD snooping will only forward multicast data to ports that wish to receive this data through the use of queries and reports produced by the requesting ports and the source of the multicast traffic.

MLD snooping is accomplished through the examination of the layer 3 part of an MLD control packet transferred between end nodes and a MLD router. When the Switch discovers that this route is requesting multicast traffic, it adds the port directly attached to it into the correct IPv6 multicast table, and begins the process of forwarding multicast traffic to that port. This entry in the multicast routing table records the port, the VLAN ID and the associated multicast IPv6 multicast group address and then considers this port to be a active listening port. The active listening ports are the only ones to receive multicast group data.

The Switch supports both MLD Snooping version 1 and MLD version 2.

MLD Control Messages

If implementing MLD snooping version 1, three types of messages are transferred between devices. These three messages are all defined by three ICMPv6 packet headers, labeled 130, 131, and 132.

1. **Multicast Listener Query, Version 1** – Similar to the IGMPv2 Host Membership Query for IPv4, and labeled as 130 in the ICMPv6 packet header, this message is sent by the router to ask if any link is requesting multicast data. There are two types of MLD query messages emitted by the router. The General Query is used to advertise all multicast addresses that are ready to send multicast data to all listening ports, and the Multicast Specific query, which advertises a specific multicast address that is also ready. These two types of messages are distinguished by a multicast destination address located in the IPv6 header and a multicast address in the Multicast Listener Query Message.

2. **Multicast Listener Report, Version 1** – Comparable to the Host Membership Report in IGMPv2, and labeled as 131 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.
3. **Multicast Listener Done** – Akin to the Leave Group Message in IGMPv2, and labeled as 132 in the ICMPv6 packet header, this message is sent by the multicast listening port stating that it is no longer interested in receiving multicast data from a specific multicast group address, therefore stating that it is "done" with the multicast data from this address. Once this message is received by the Switch, it will no longer forward multicast traffic from a specific multicast group address to this listening port.

If implementing MLD snooping version 2, two types of messages are transferred between devices. The two messages are defined by two ICMPv6 packet headers, labeled 130 and 143.

1. **Multicast Listener Query, Version 2** – Similar to the IGMPv3 Membership Query for IPv4, and labeled as 130 in the ICMPv6 packet header, this message is sent by the router to ask if any link is requesting multicast data. With MLD snooping version 2, there are three types of MLD query messages emitted by the router, as described below:
    - The router sends a General Query message to learn which multicast addresses have listeners on an attached link. In a General Query, both the Multicast Address field and the Number of Sources field are set to zero.
    - The router sends a Multicast Address Specific Query message to learn if a particular multicast address has any listeners on an attached link. In a Multicast Address Specific Query, the Multicast Address field contains the multicast address that the router is interested in, while the Number of Sources field is set to zero.
    - The router sends a Multicast Address and Source Specific Query to learn if any of the sources from the specified list for the particular multicast address has any listeners on an attached link or not. In a Multicast Address and Source Specific Query the Multicast Address field contains the multicast address that the router is interested in, while the Source Address field(s) contain(s) the source address(es) that the router is interested in.
2. **Multicast Listener Report, Version 2** - Comparable to the Host Membership Report in IGMPv3, and labeled as 143 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.

This window is used to enable MLD Snooping on the Switch and to configure the settings for MLD snooping. To enable the MLD Snooping State, click the Enable radio button under MLD Snooping Global Settings and click **Apply**.

To view this window, click **L2 Features > MLD Snooping Settings**:

Figure 3 - 36. MLD Snooping Settings window

To configure the settings for an existing entry click the corresponding **Edit** button which will display the following window.

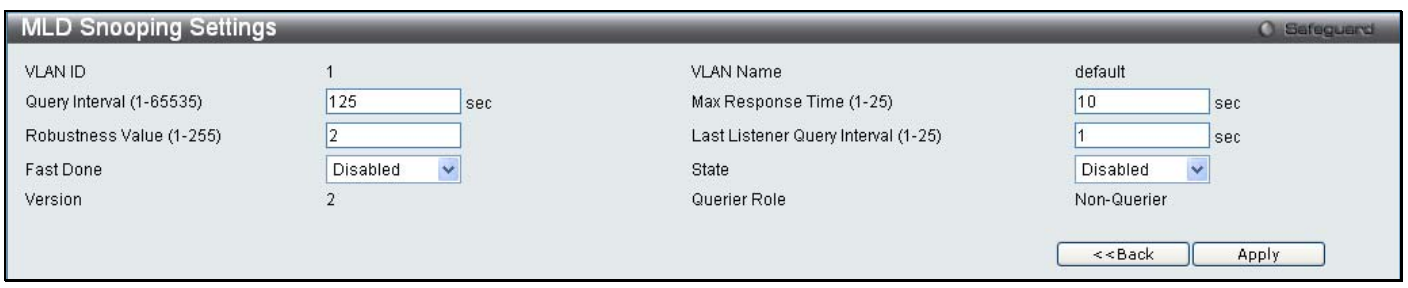


Figure 3 - 37. MLD Snooping Settings (Edit) window

The following parameters may be viewed or modified:

Parameter	Description
VLAN ID	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN for which the user wishes to modify the MLD Snooping Settings.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN for which the user wishes to modify the MLD Snooping Settings.
Query Interval (1-65535)	The Query Interval field is used to set the time (in seconds) between transmitting MLD queries. Entries between *1* and *65535* seconds are allowed. The default is *125*.
Max Response Time (1-25)	This determines the maximum amount of time in seconds to wait for reports from members. The Max Response Time field allows an entry between 1 and 25 (seconds). The default is *10*.
Robustness Value (1-255)	Adjust this variable according to expected packet loss. If packet loss on the VLAN is expected to be high, the Robustness Variable should be increased to accommodate increased packet loss. This entry field allows an entry of *1* to *255*. The default is *2*.
Last Listener Query Interval (1-25)	This field specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. The default is *1*.
Fast Done	This parameter allows the user to enable the Fast Leave function. *Enabled*, this function will allow members of a multicast group to leave the group immediately (without the implementation of the Last Listener Query Interval) when an MLD Leave Report Packet is received by the Switch. The default is *Disabled*.
State	Select *Enabled* to implement MLD Snooping. This field is *Disabled* by default.
Version	The read-only field displays the MLD version used on the Switch, 2.
Querier Role	This read-only field describes the behavior of the Switch for sending query packets. Querier will denote that the Switch is sending out MLD query packets. Non-Querier will denote that the Switch is not sending out MLD query packets.

Click **Apply** to implement any changes made and **<<Back** to return to the initial **MLD Snooping Settings** window.

To modify the MLD Snooping Router Port Settings, click on the hyperlinked Modify Router Port, which will show the following window for the user to configure:

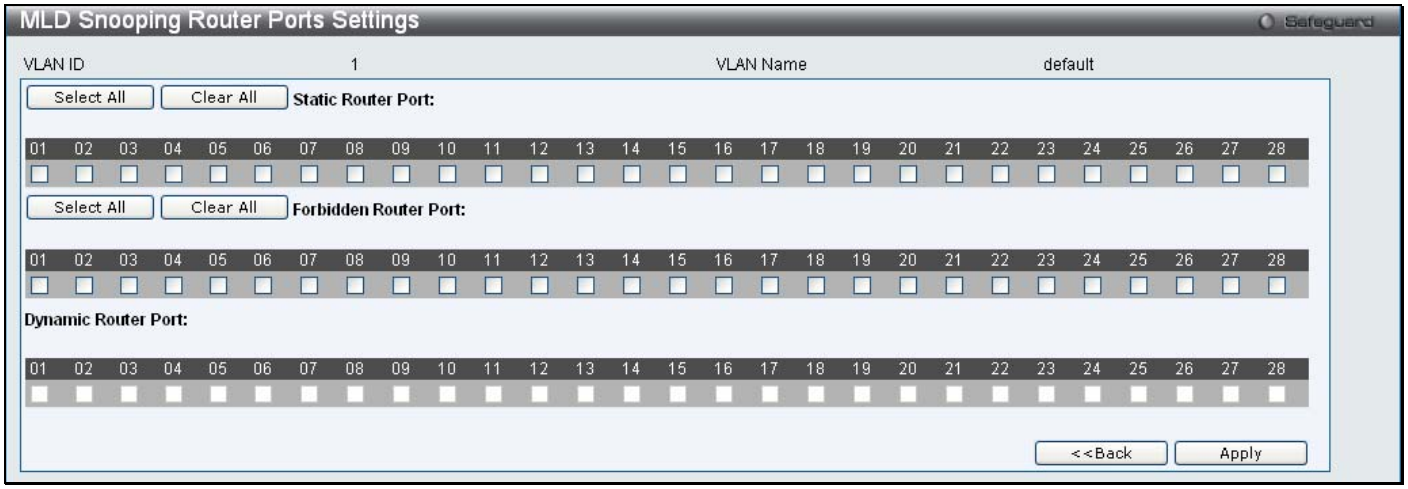


Figure 3 - 38. MLD Snooping Router Ports Settings window

Select the desired router ports and then click **Apply** to implement any changes made. To select either all of the static router ports or all of the forbidden router ports, click the corresponding **Select All** button. To clear either all of the selected static router ports or all of the selected forbidden router ports, click the corresponding **Clear All** button. Click **<<Back** to return to the **MLD Snooping Settings** window.

Port Mirror

The Switch allows you to copy frames transmitted and received on a port and redirect the copies to another port. You can attach a monitoring device to the mirrored port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes.

To view this window, click **Layer 2 Features > Port Mirror**:

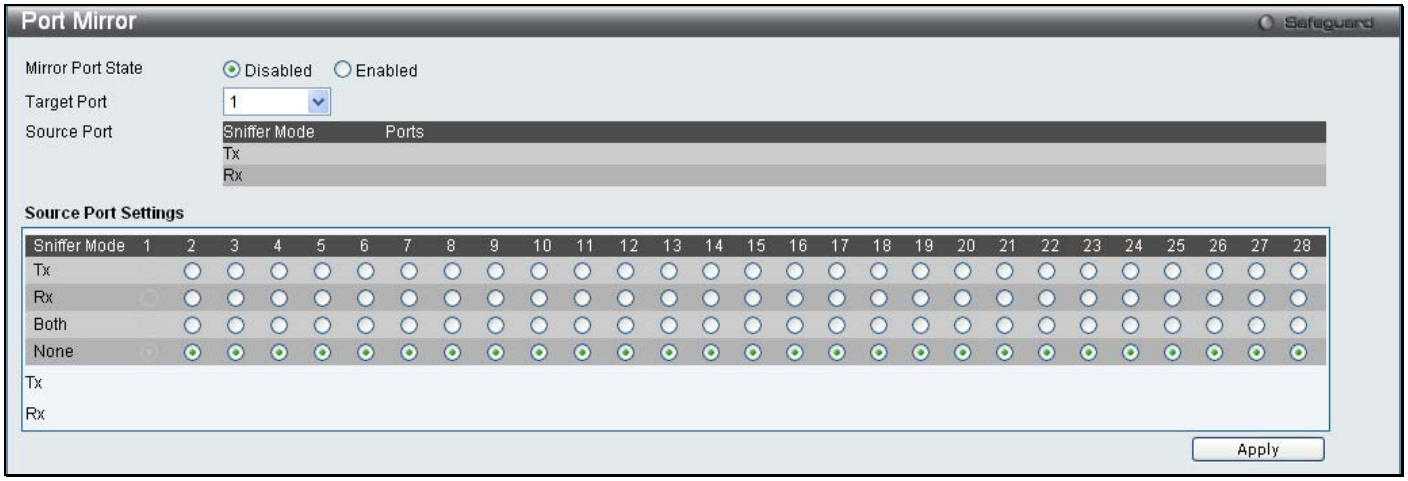


Figure 3 - 39. Port Mirror window

To configure a mirror port:

1. Change the status to Enabled.
2. Select the Target Port, which receives the copies from the source port.
3. Select the Source Port from where the frames come from.
4. Click **Apply** to let the changes take effect.

NOTE: You cannot mirror a fast port onto a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies. Also, the target port for the mirroring cannot be a member of a trunk group. Please note a target port and a source port cannot be the same port.

Loopback Detection Settings

The Loopback Detection function is used to detect the loop created by a specific port. This feature is used to temporarily shutdown a port on the Switch when a CTP (Configuration Testing Protocol) packet has been looped back to the Switch. When the Switch detects CTP packets received from a port, it signifies a loop on the network. The Switch will automatically block the port and send an alert to the administrator. The Loopback Detection port will restart (change to discarding state) when the Loopback Detection Recover Time times out. The Loopback Detection function can be implemented on a range of ports at a time. The user may enable or disable this function using the pull-down menu.

To view this window, click **L2 Features > Loopback Detection Settings**:

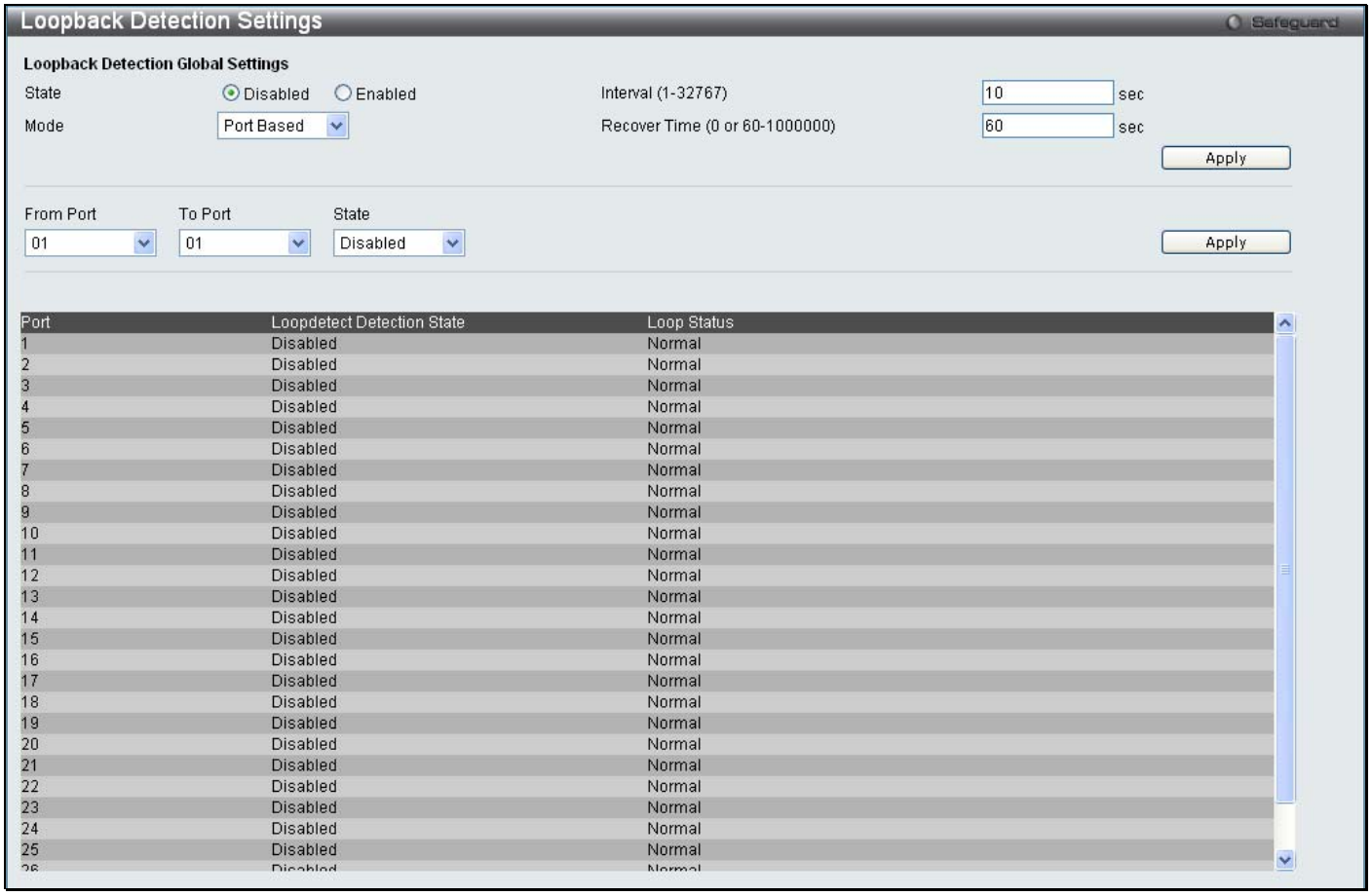


Figure 3 - 40. Loopback Detection Settings window

Parameter	Description
State	Use the drop-down menu to enable or disable loopback detection. The default is *Disabled.*
Interval (1-32767)	Set a loop-detect Interval between *1* and *32767* seconds. The default is *10* seconds.
Mode	This read-only field displays Port Based.
Recover Time (0 or 60-1000000)	Time allowed (in seconds) for recovery when a loopback is detected. The Loop-detect Recover Time can be set at *0* seconds, or *60* to *1000000* seconds. Entering *0* will disable the Loopdetect Recover Time. The default is *60* seconds.
From Port	Use the drop-down menu to select a beginning port number.
To Port	Use the drop-down menu to select an ending port number.
State	Use the drop-down menu to toggle between *Enabled* and *Disabled.*

Click **Apply** to implement changes made.

Spanning Tree

This Switch supports three versions of the Spanning Tree Protocol: STP, Rapid STP, and MSTP. STP will be familiar to most networking professionals. However, since RSTP and MSTP have been recently introduced to D-Link managed Ethernet switches, a brief introduction to the technology is provided below followed by a description of how to set up STP, RSTP, and MSTP.

802.1Q-2005 MSTP

Multiple Spanning Tree Protocol, or MSTP, is a standard defined by the IEEE community that allows multiple VLANs to be mapped to a single spanning tree instance, which will provide multiple pathways across the network. Therefore, these MSTP configurations will balance the traffic load, preventing wide scale disruptions when a single spanning tree instance fails. This will allow for faster convergences of new topologies for the failed instance. Frames designated for these VLANs will be processed quickly and completely throughout interconnected bridges utilizing any of the three spanning tree protocols (STP, RSTP or MSTP).

This protocol will also tag BPDU packets so receiving devices can distinguish spanning tree instances, spanning tree regions and the VLANs associated with them. An MSTI ID will classify these instances. MSTP will connect multiple spanning trees with a Common and Internal Spanning Tree (CIST). The CIST will automatically determine each MSTP region, its maximum possible extent and will appear as one virtual bridge that runs a single spanning tree. Consequentially, frames assigned to different VLANs will follow different data routes within administratively established regions on the network, continuing to allow simple and full processing of frames, regardless of administrative errors in defining VLANs and their respective spanning trees.

Each switch utilizing the MSTP on a network will have a single MSTP configuration that will have the following three attributes:

1. A configuration name defined by an alphanumeric string of up to 32 characters (defined in the **MST Configuration Identification** window in the Configuration Name field).
2. A configuration revision number (named here as a Revision Level and found in the **MST Configuration Identification** window) and;
3. A 4094-element table (defined here as a VID List in the **MST Configuration Identification** window), which will associate each of the possible 4094 VLANs supported by the Switch for a given instance.

To utilize the MSTP function on the Switch, three steps need to be taken:

1. The Switch must be set to the MSTP setting (found in the **STP Bridge Global Settings** window in the STP Version field)
2. The correct spanning tree priority for the MSTP instance must be entered (defined here as a Priority in the **MSTI Config Information** window when configuring MSTI ID settings).
3. VLANs that will be shared must be added to the MSTP Instance ID (defined here as a VID List in the **MST Configuration Identification** window when configuring an MSTI ID settings).

Rapid Spanning Tree

The Switch implements three versions of the Spanning Tree Protocol, the Multiple Spanning Tree Protocol (MSTP) as defined by the IEEE 802.1Q-2005, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1D-2004 specification and a version compatible with the IEEE 802.1D-1998 STP. RSTP can operate with legacy equipment implementing IEEE 802.1D-1998, however the advantages of using RSTP will be lost.

The Rapid Spanning Tree Protocol (RSTP) evolved from the STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations, in particular, certain Layer 3 functions that are increasingly handled by Ethernet switches. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

Port Transition States

An essential difference between the three protocols is in the way ports transition to a forwarding state and in the way this transition relates to the role of the port (forwarding or not forwarding) in the topology. MSTP and RSTP combine the transition states disabled, blocking and listening used in STP and creates a single state Discarding. In either case, ports do not forward packets. In the STP port transition states disabled, blocking or listening or in the RSTP/MSTP port state discarding, there is no functional difference, the port is not active in the network topology. The table below compares how the three protocols differ regarding the port state transition.

All three protocols calculate a stable topology in the same way. Every segment will have a single path to the root bridge. All bridges listen for BPDU packets. However, BPDU packets are sent more frequently - with every Hello packet. BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges is sensitive to the status of the link. Ultimately this difference results in faster detection of failed links, and thus faster topology adjustment. A drawback of STP is this absence of immediate feedback from adjacent bridges.

MSTP	RSTP	STP	Forwarding	Learning
Disabled	Disabled	Disabled	No	No
Discarding	*Discarding*	*Blocking*	No	No
Discarding	*Discarding*	*Listening*	No	No
Learning	*Learning*	*Learning*	No	**Yes**
Forwarding	**Forwarding**	**Forwarding**	**Yes**	**Yes**

Table 3 - 1. Comparing Port States

RSTP is capable of a more rapid transition to a forwarding state - it no longer relies on timer configurations - RSTP compliant bridges are sensitive to feedback from other RSTP compliant bridge links. Ports do not need to wait for the topology to stabilize before transitioning to a forwarding state. In order to allow this rapid transition, the protocol introduces two new variables: the edge port and the point-to-point (P2P) port.

Edge Port

The edge port is a configurable designation used for a port that is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single workstation. Ports that are designated as edge ports transition to a forwarding state immediately without going through the listening and learning states. An edge port loses its status if it receives a BPDU packet, immediately becoming a normal spanning tree port.

P2P Port

A P2P port is also capable of rapid transition. P2P ports may be used to connect to other bridges. Under RSTP/MSTP, all ports operating in full-duplex mode are considered to be P2P ports, unless manually overridden through configuration.

STP/RSTP/MSTP Compatibility

MSTP or RSTP can interoperate with legacy equipment and is capable of automatically adjusting BPDU packets to STP format when necessary. However, any segment using STP will not benefit from the rapid transition and rapid topology change detection of MSTP or RSTP. The protocol also provides for a variable used for migration in the event that legacy equipment on a segment is updated to use RSTP or MSTP.

The Spanning Tree Protocol (STP) operates on two levels:

1. On the switch level, the settings are globally implemented.
2. On the port level, the settings are implemented on a per user-defined group of ports basis.

STP Bridge Global Settings

To open the following window, click **L2 features > Spanning Tree > STP Bridge Global Settings**:

Figure 3 - 41. STP Bridge Global Settings window

The following parameters can be set:

Parameter	Description
STP State	Use the radio buttons to enable or disable the STP Status.
STP Version	Use the pull-down menu to choose the desired version of STP to be implemented on the Switch. There are three choices: *STP* - Select this parameter to set the Spanning Tree Protocol (STP) globally on the switch. *RSTP* - Select this parameter to set the Rapid Spanning Tree Protocol (RSTP) globally on the Switch. *MSTP* – Select this parameter to set the Multiple Spanning Tree Protocol (MSTP) globally on the Switch.
Forwarding BPDU	This field can be *Enabled* or *Disabled.* When *Enabled,* it allows the forwarding of STP BPDU packets from other network devices. The default is *Enabled*.
Bridge Max Age (6-40)	The Max Age may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your switch has the lowest Bridge Identifier, it will become the Root Bridge. The user may choose a time between *6* and *40* seconds. The default value is *20*.
Bridge Forward Delay (4-30)	The Forward Delay can be from *4* to *30* seconds. Any port on the Switch spends this time in the listening state while moving from the blocking state to the forwarding state.
Tx Hold Count (1-10)	Used to set the maximum number of Hello packets transmitted per interval. The count can be specified from *1* to *10*. The default is *6.*
Max Hops (6-40)	Used to set the number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BPDU packet and the information held for the port will age out. The user may set a hop count from *6* to *40*. The default is *20*.

Click **Apply** to implement changes made.

NOTE: The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur. Observe the following formulas when setting the above parameters:

Max. Age ≤ 2 x (Forward Delay - 1 second)

Max. Age ≥ 2 x (Hello Time + 1 second)

STP Port Settings

STP can be set up on a port per port basis.

To view the following window, click **L2 Features > Spanning Tree > STP Port Settings**:

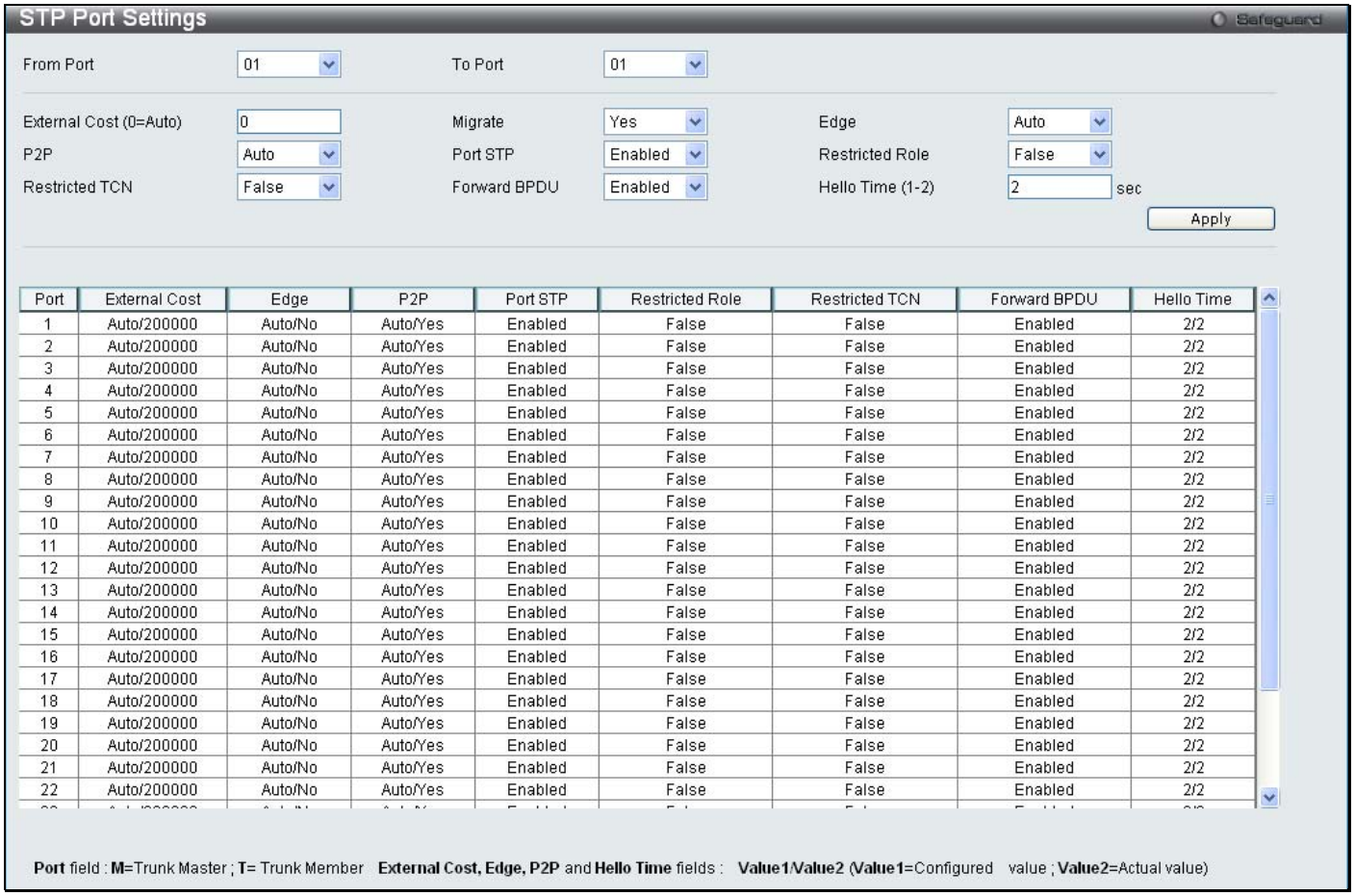

STP Port Settings
Safeguard
From Port 01
To Port 01
External Cost (0=Auto) 0
Migrate Yes
Edge Auto
P2P Auto
Port STP Enabled
Restricted Role False
Restricted TCN False
Forward BPDU Enabled
Hello Time (1-2) 2 sec
Apply
Port | External Cost | Edge | P2P | Port STP | Restricted Role | Restricted TCN | Forward BPDU | Hello Time
1 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
2 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
3 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
4 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
5 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
6 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
7 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
8 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
9 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
10 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
11 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
12 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
13 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
14 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
15 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
16 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
17 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
18 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
19 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
20 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
21 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
22 Auto/200000 Auto/No Auto/Yes Enabled False False Enabled 2/2
Port field : M=Trunk Master ; T= Trunk Member External Cost, Edge, P2P and Hello Time fields : Value1/Value2 (Value1=Configured value ; Value2=Actual value)

Figure 3 - 42. STP Port Settings window

In addition to setting Spanning Tree parameters for use on the switch level, the Switch allows for the configuration of groups of ports, each port-group of which will have its own spanning tree, and will require some of its own configuration settings. An STP Group will use the switch-level parameters entered above, with the addition of Port Priority and Port Cost.

An STP Group spanning tree works in the same way as the switch-level spanning tree, but the root bridge concept is replaced with a root port concept. A root port is a port of the group that is elected based on port priority and port cost, to be the connection to the network for the group. Redundant links will be blocked, just as redundant links are blocked on the switch level.

The STP on the switch level blocks redundant links between switches (and similar network devices). The port level STP will block redundant links within an STP Group.

It is advisable to define an STP Group to correspond to a VLAN group of ports.

The following fields can be set:

Parameter	Description
From Port/To Port	A consecutive group of ports may be configured starting with the selected port.
External Cost (0=Auto)	External Cost - This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is *0* (auto). *0 (auto)* - Setting *0* for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = *200000*. Gigabit port = *20000*. *value 1-200000000* - Define a value between *1* and *200000000* to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.
Migrate	Setting this parameter as *Yes* will set the ports to send out BPDU packets to other bridges, requesting information on their STP setting If the Switch is configured for RSTP, the port will be capable to migrate from 802.1D STP to 802.1w RSTP. Migration should be set as yes on ports connected to network stations or segments that are capable of being upgraded to 802.1w RSTP on all or some portion of the segment.
Edge	Choosing the *True* parameter designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received, it automatically loses edge port status. Choosing the *Auto* parameter will indicate that the port will be able to automatically enable edge port status if needed.
P2P	Choosing the *True* parameter indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports, however they are restricted in that a P2P port must operate in full-duplex. Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A p2p value of *false* indicates that the port cannot have p2p status. *Auto* allows the port to have p2p status whenever possible and operate as if the p2p status were true. If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were *False*. The default setting for this parameter is *True*. The default value *True* is equivalent to the *Auto* value.
Port STP	Allows STP to be *Enabled* or *Disabled* for the ports.
Restricted Role	Toggle between *True* and *False* to set the restricted role state of the packet. The default value is *False*.
Restricted TCN	Toggle between *True* and *False* to set the restricted TCN of the packet. The default value is *False*.
Forward BPDU	This field can be *Enabled* or *Disabled.* When *Enabled,* it allows the forwarding of STP BPDU packets from other network devices. The default is *Enabled*.
Hello Time (1–2)	The Hello Time can be set from *1* to *2* seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. The default value is *2*.

Click **Apply** to implement changes made.

MST Configuration Identification

The following windows in the MST Configuration Identification section allow the user to configure a MSTI instance on the Switch. These settings will uniquely identify a multiple spanning tree instance set on the Switch. The Switch initially possesses one *CIST* or Common Internal Spanning Tree of which the user may modify the parameters for but cannot change the MSTI ID for, and cannot be deleted.

To view this window, click **L2 Features > Spanning Tree > MST Configuration Identification**:

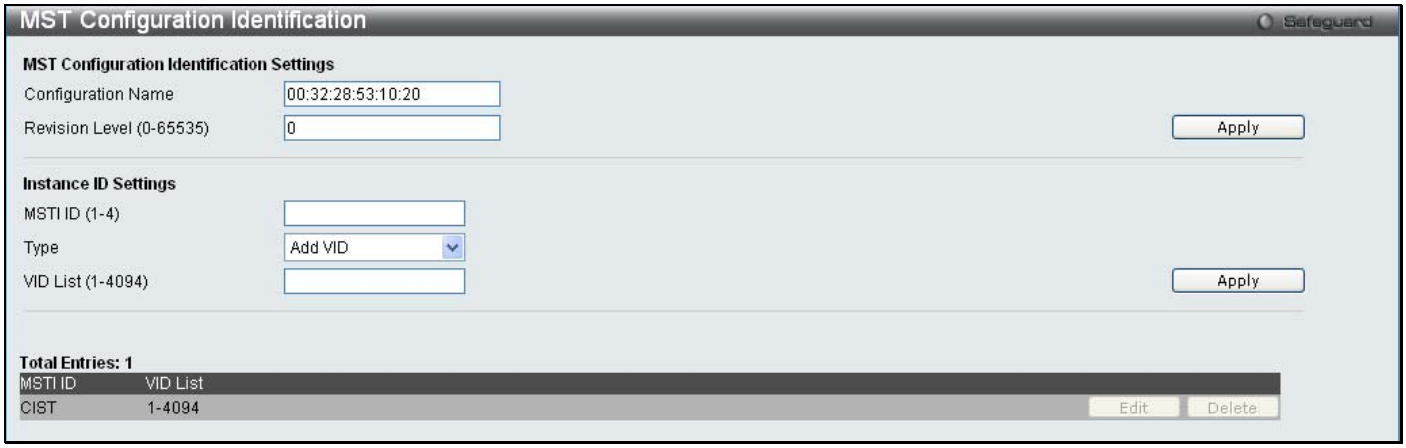


Figure 3 - 43. MST Configuration Identification window

The window above contains the following information:

Parameter	Description
Configuration Name	A previously configured name set on the Switch to uniquely identify the MSTI (Multiple Spanning Tree Instance). If a configuration name is not set, this field will show the MAC address to the device running MSTP. This field can be set in the **STP Bridge Global Settings** window.
Revision Level (0-65535)	This value, along with the Configuration Name will identify the MSTP region configured on the Switch. The user may choose a value between *0* and *65535* with a default setting of *0*.
MSTI ID (1-4)	This field shows the MSTI IDs currently set on the Switch. This field will always have the CIST MSTI, which may be configured but not deleted. Clicking the hyperlinked name will open a new window for configuring parameters associated with that particular MSTI.
Type	This field allows the user to choose a desired method for altering the MSTI settings. The user has two choices. *Add VID* - Select this parameter to add VIDs to the MSTI ID, in conjunction with the VID List parameter. *Remove VID* - Select this parameter to remove VIDs from the MSTI ID, in conjunction with the VID List parameter.
VID List (1-4094)	This field displays the VLAN IDs associated with the specific MSTI.

Click **Apply** for changes to take affect.

STP Instance Settings

The following window displays MSTIs currently set on the Switch.

To view the following table, click **L2 Features > Spanning Tree > STP Instance Settings**:

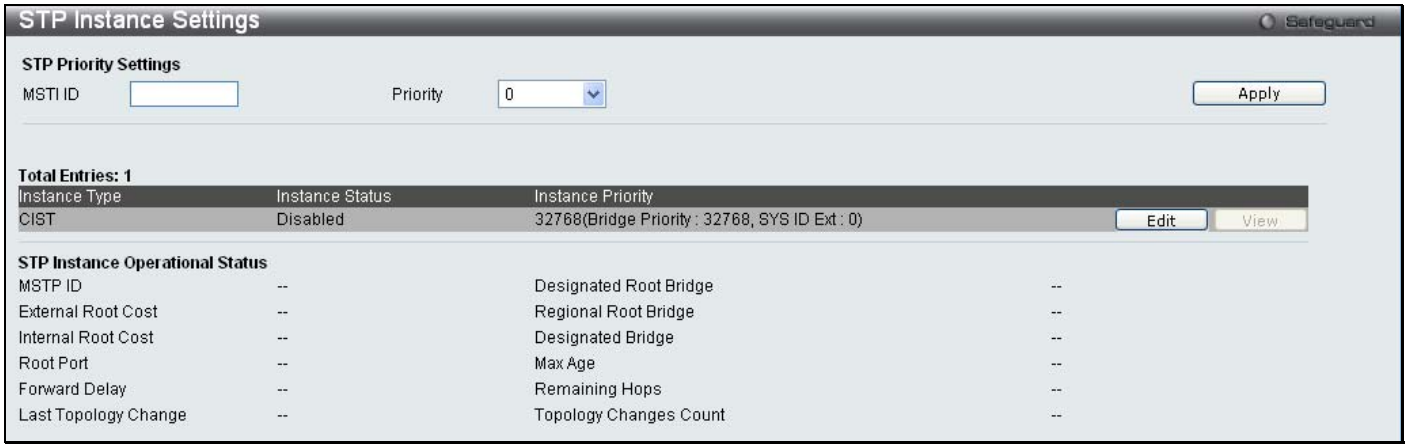


Figure 3 - 44. STP Instance Settings window

The following information can be set:

Parameter	Description
MSTI ID	Displays the MSTI ID of the instance being modified. An entry of *0* in this field denotes the CIST (default MSTI).
Priority	Enter the new priority in the Priority field. The user may set a priority value between *0* and *61440*.

To modify an entry, click the **Edit** button.

To see the STP Instance Operational Status of a previously configured setting, click **View**. The following window will be displayed:

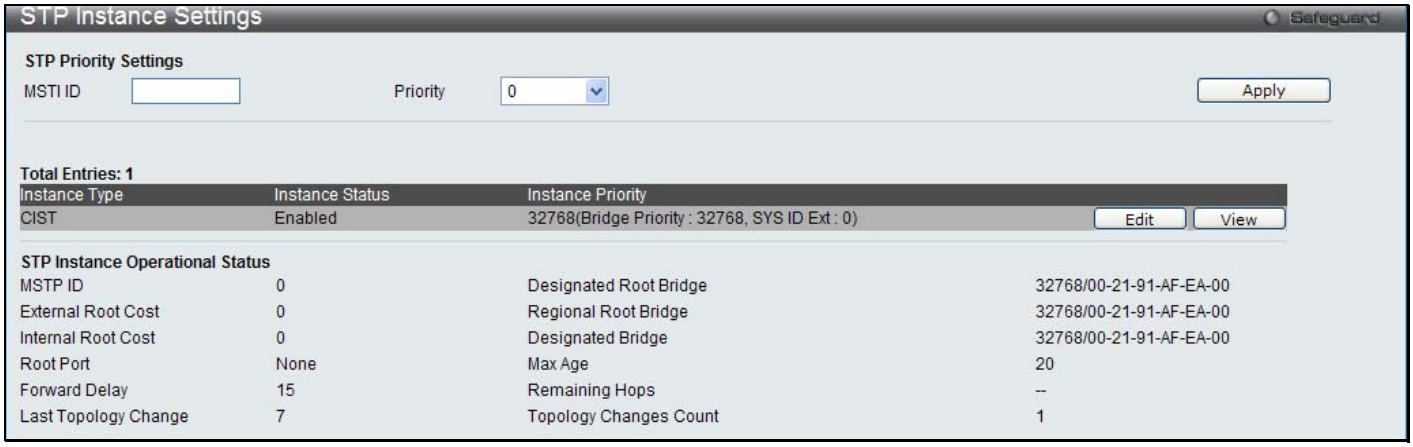


Figure 3 - 45. STP Instance Settings - View window

MSTP Port Information

This window displays the current MSTP Port Information and can be used to update the port configuration for an MSTI ID. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for interfaces to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked. Remember that lower priority values mean higher priorities for forwarding packets.

To view the following window, click **L2 Features > Spanning Tree > MSTP Port Information**:

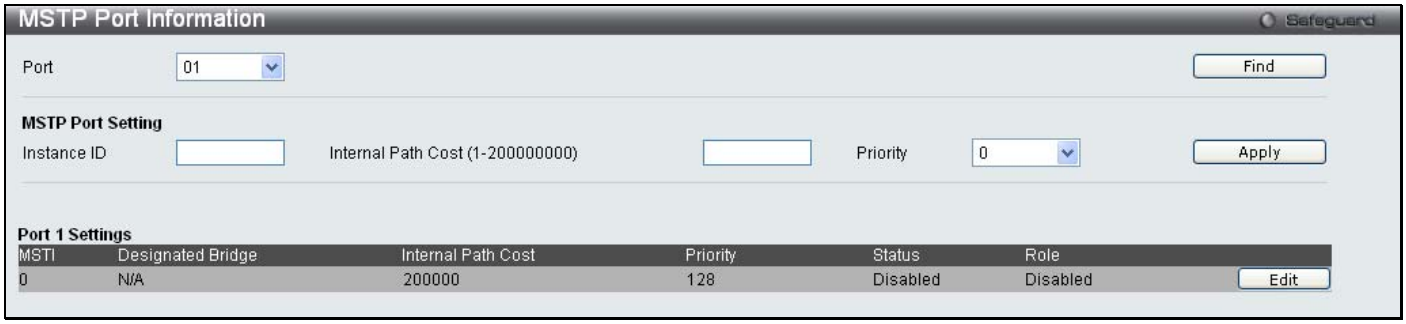


Figure 3 - 46. MSTP Port Information window

The following parameters can be viewed or set:

Parameter	Description
Port	Use the drop-down menu to select a port.
Instance ID	Displays the MSTI ID of the instance being configured. An entry of *0* in this field denotes the CIST (default MSTI).
Internal Path Cost (1-200000000)	This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within a STP instance. A lower Internal cost represents a quicker transmission.
Priority	Select a value between *0* and *240* to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority.

Click **Apply** to implement changes made.

Forwarding & Filtering

This folder contains windows for Unicast Forwarding and Multicast Forwarding.

Unicast Forwarding Settings

To view this window, click **L2 Features > Forwarding & Filtering > Unicast Forwarding Settings**:

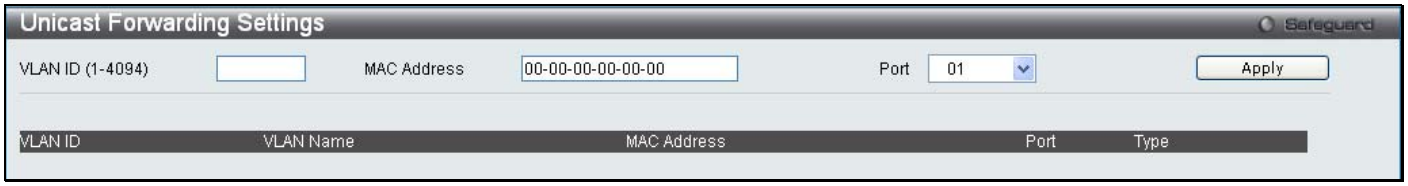


Figure 3 - 47. Unicast Forwarding Settings window

To add or edit an entry, define the following parameters and then click **Add/Modify**:

Parameter	Description
VLAN ID (1-4094)	The VLAN ID number of the VLAN on which the above Unicast MAC address resides.
MAC Address	The MAC address to which packets will be statically forwarded. This must be a unicast MAC address.
Port	Select the port number on which the MAC address entered above resides.
VLAN Name	The VLAN Name associated with the subnet.

Click **Apply** to implement the changes made. The new entries will be displayed on the bottom half of the window.

Multicast Forwarding Settings

To view this window, click **L2 Features > Forwarding & Filtering > Multicast Forwarding Settings**:

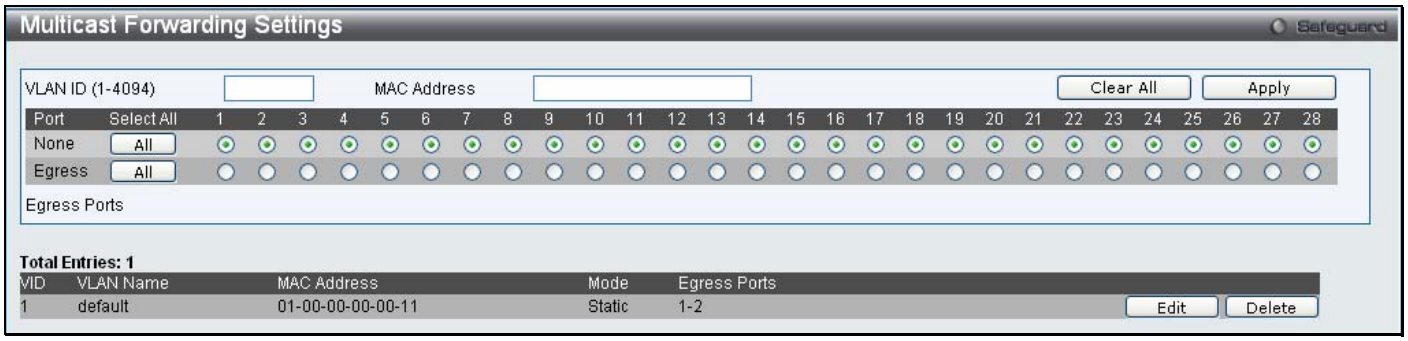


Figure 3 - 48. Multicast Forwarding Settings window

The following parameters can be set:

Parameter	Description
VLAN ID (1-4094)	The VLAN ID of the VLAN to which the corresponding MAC address belongs.
MAC Address	The MAC address that will be added to the multicast forwarding table.
Port Settings	Allows the selection of ports that will be members of the static multicast group. The options are: *None* - No restrictions on the port dynamically joining the multicast group. When None is chosen, the port will not be a member of the static multicast group. *Egress* - The port is a static member of the multicast group. Click **All** to choose either all of the ports selected as None or all of the ports selected as Egress. Click **Clear All** to clear all the settings at the top of this window.

Click **Apply** to implement the changes made. To delete an entry in the static multicast forwarding table, click the corresponding **Delete** button. To modify an entry in the static multicast forwarding table, click the corresponding **Edit** button and make the desired changes at the top of the window before clicking the **Apply** button.

Multicast Filtering Mode

Users can configure the multicast filtering mode.

To view this window, click **L2 Features > Forwarding & Filtering > Multicast Filtering Mode**:

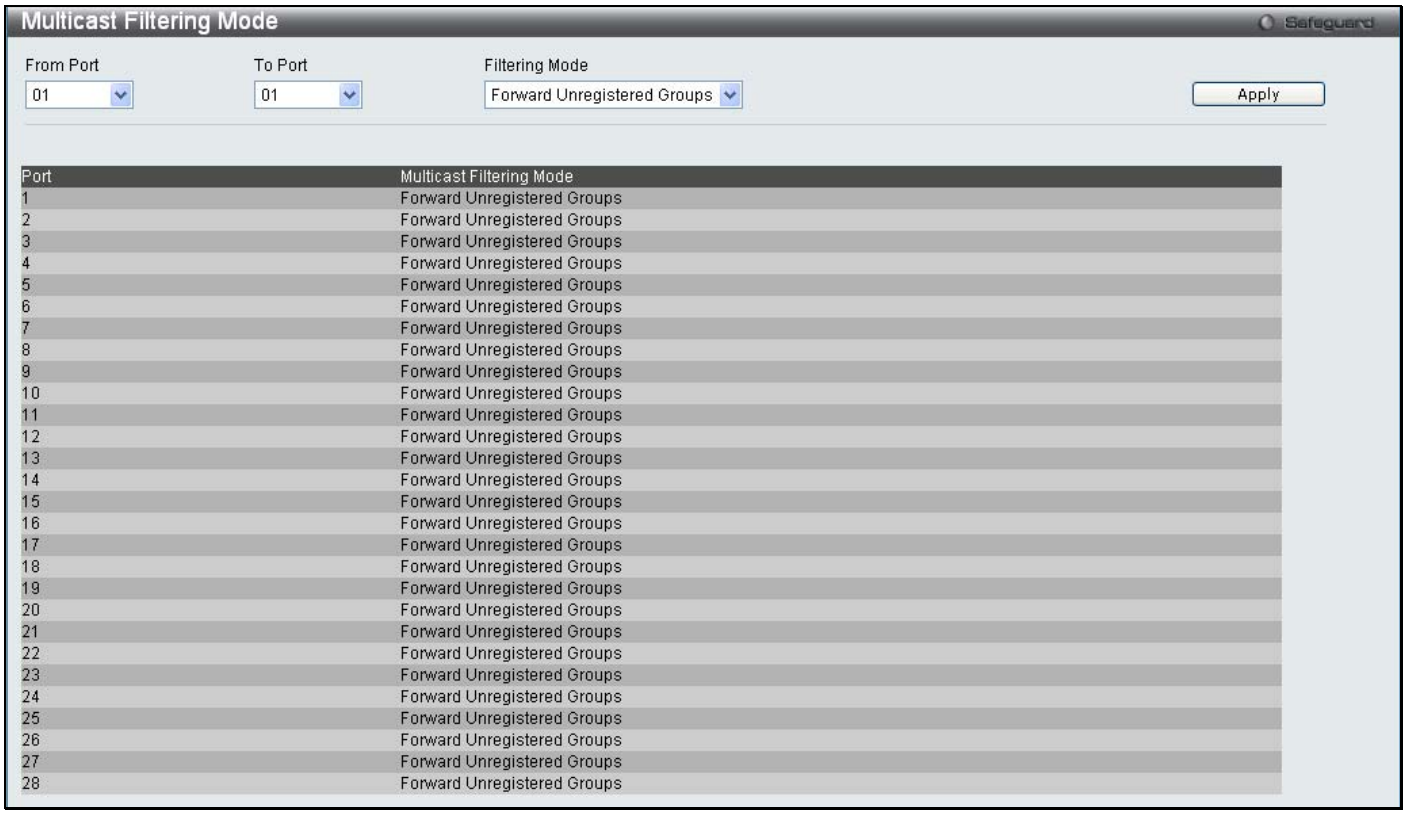


Figure 3 - 49. Multicast Filtering Mode window

The following parameters can be set:

Parameter	Description
From Port/To Port	The range of ports to be configured.
Filtering Mode	This drop-down menu instructs the Switch what action to take when it receives a multicast packet that requires forwarding to a port. *Forward Unregistered Groups* – This will instruct the Switch to forward a multicast packet whose destination is an unregistered multicast group residing within the range of ports specified above. *Filter Unregistered Groups* – This will instruct the Switch to filter any multicast packets whose destination is an unregistered multicast group residing within the range of ports specified above..

Click **Apply** to implement the changes made.

LLDP

The Link Layer Discovery Protocol (LLDP) allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN. The major capabilities provided by this system is that it incorporates the station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the station's point of attachment to the IEEE 802 LAN required by those management entity or entities.

The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) through a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP Global Settings

To view this window, click **L2 Features > LLDP > LLDP Global Settings**:

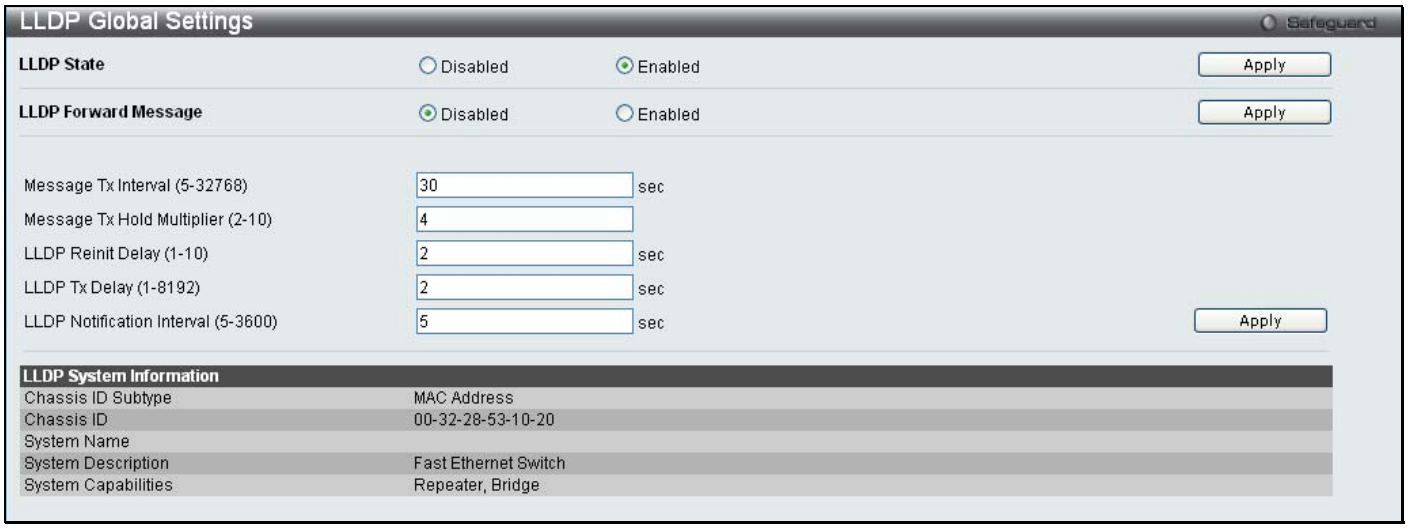


Figure 3 - 50. LLDP Global Settings window

The following parameters can be set:

Parameter	Description
LLDP State	Used to enable or disable LLDP on the Switch.
LLDP Forward Message	When LLDP is Disabled this function controls the LLDP packet forwarding message based on individual ports. If LLDP is enabled on a port it will flood the LLDP packet to all ports that have the same port VLAN and will advertise to other stations attached to the same IEEE 802 LAN.
Message Tx Interval (5-32768)	This interval controls how often active ports retransmit advertisements to their neighbors. To change the packet transmission interval, enter a value in seconds (*5* to *32768*).
Message Tx Hold Multiplier (2-10)	This function calculates the Time-to-Live for creating and transmitting the LLDP advertisements to LLDP neighbors by changing the multiplier used by an LLDP Switch. When the Time-to-Live for an advertisement expires the advertised data is then deleted from the neighbor Switch's MIB.
LLDP Reinit Delay (1-10)	The LLDP reinitialization delay interval is the minimum time that an LLDP port will wait before reinitializing after receiving an LLDP disable command. To change the LLDP Reinit Delay, enter a value in seconds (*1* to *10*).
LLDP Tx Delay (1-8192)	LLDP TX Delay allows the user to change the minimum time delay interval for any LLDP port which will delay advertising any successive LLDP advertisements due to change in the LLDP MIB content. To change the LLDP TX Delay, enter a value in seconds (*1* to *8192*).
LLDP Notification Interval (5-3600)	LLDP Notification Interval is used to send notifications to configured SNMP trap receiver(s) when an LLDP change is detected in an advertisement received on the port from an LLDP neighbor. To set the LLDP Notification Interval, enter a value in seconds (*5* to *3600*).

Click **Apply** to implement changes made.

LLDP Port Settings

To view this window, click **L2 Features > LLDP > LLDP Port Settings**:

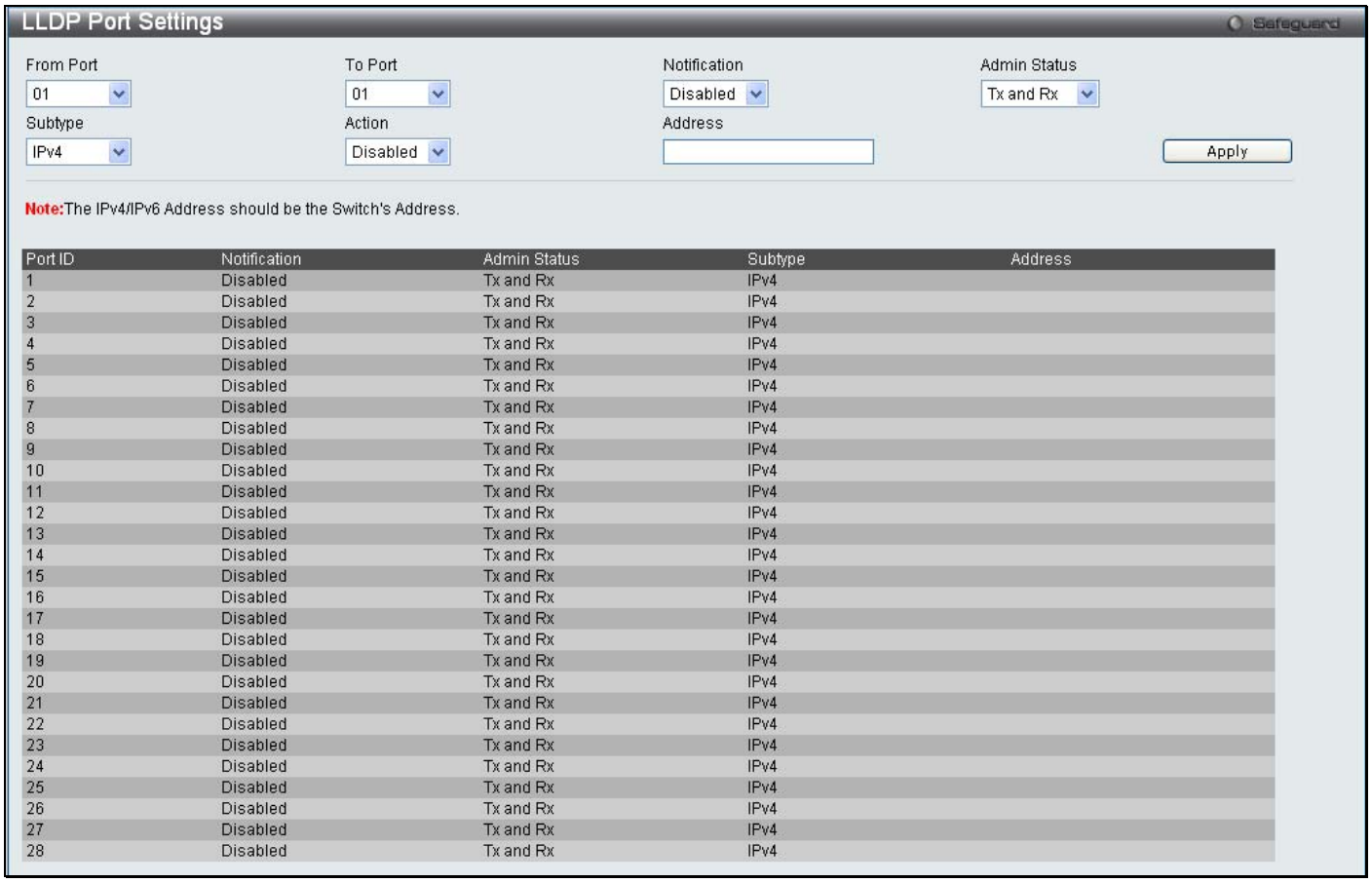

LLDP Port Settings
Safeguard
From Port
01
To Port
01
Notification
Disabled
Admin Status
Tx and Rx
Subtype
IPv4
Action
Disabled
Address
Apply
Note:The IPv4/IPv6 Address should be the Switch's Address.
Port ID Notification Admin Status Subtype Address
1 Disabled Tx and Rx IPv4
2 Disabled Tx and Rx IPv4
3 Disabled Tx and Rx IPv4
4 Disabled Tx and Rx IPv4
5 Disabled Tx and Rx IPv4
6 Disabled Tx and Rx IPv4
7 Disabled Tx and Rx IPv4
8 Disabled Tx and Rx IPv4
9 Disabled Tx and Rx IPv4
10 Disabled Tx and Rx IPv4
11 Disabled Tx and Rx IPv4
12 Disabled Tx and Rx IPv4
13 Disabled Tx and Rx IPv4
14 Disabled Tx and Rx IPv4
15 Disabled Tx and Rx IPv4
16 Disabled Tx and Rx IPv4
17 Disabled Tx and Rx IPv4
18 Disabled Tx and Rx IPv4
19 Disabled Tx and Rx IPv4
20 Disabled Tx and Rx IPv4
21 Disabled Tx and Rx IPv4
22 Disabled Tx and Rx IPv4
23 Disabled Tx and Rx IPv4
24 Disabled Tx and Rx IPv4
25 Disabled Tx and Rx IPv4
26 Disabled Tx and Rx IPv4
27 Disabled Tx and Rx IPv4
28 Disabled Tx and Rx IPv4

Figure 3 - 51. LLDP Port Settings window

The following parameters can be set:

Parameter	Description
From Port/To Port	Use the pull-down menu to select a range of ports to be configured.
Notification	Use the pull-down menu to Enable or Disable the status of the LLDP notification. This function controls the SNMP trap, however it cannot implement traps on SNMP when the notification is disabled.
Admin Status	This functions controls the local LLDP agent and allows it to send and receive LLDP frames on the ports.This option contains *Tx*, *Rx*, *Tx and Rx* or *Disabled*. *Tx*: the local LLDP agent can only transmit LLDP frames. *Rx*: the local LLDP agent can only receive LLDP frames. *Tx and Rx*: the local LLDP agent can both transmit and receive LLDP frames. *Disabled*: the local LLDP agent can neither transmit nor receive LLDP frames. The defaut value is *Tx and Rx*.
Subtype	This read-only field displays IPv4, the type of the IP address.
Action	Used to *Enable* or *Disable* the advertise management address function base port.
Address	The address must be the management IP-address. For multi IP-addresses, you can enter any IP or create a new IP interface that you want to add.

Click **Apply** to implement changes made.

LLDP Basic TLVs Settings

This window is used to enable the settings for the Basic TLVs Settings.

To view this window, click **L2 Features > LLDP > LLDP Basic TLVs Settings**:

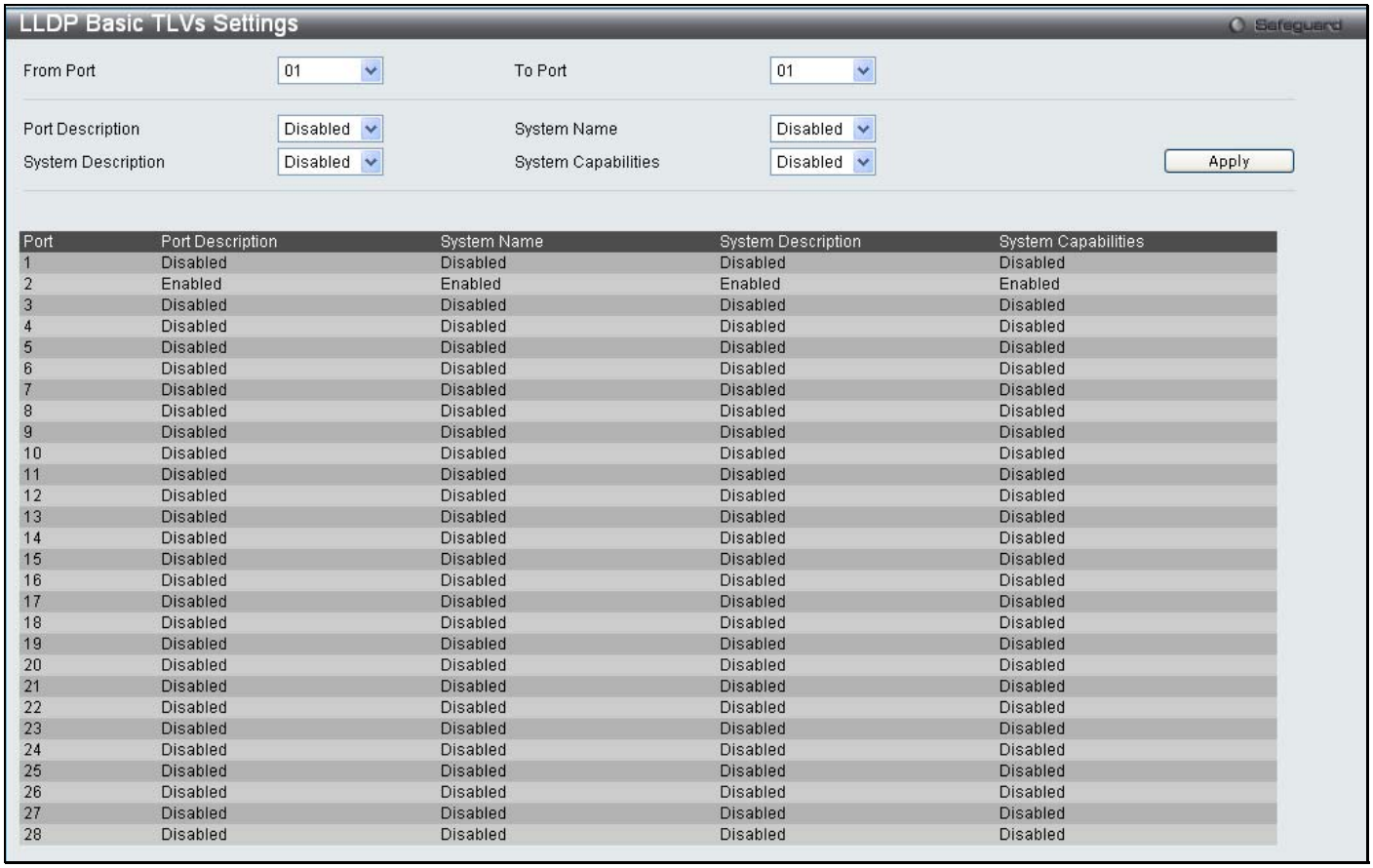

LLDP Basic TLVs Settings
Safeguard
From Port 01
To Port 01
Port Description Disabled
System Name Disabled
System Description Disabled
System Capabilities Disabled
Apply
Port Port Description System Name System Description System Capabilities
1 Disabled Disabled Disabled Disabled
2 Enabled Enabled Enabled Enabled
3 Disabled Disabled Disabled Disabled
4 Disabled Disabled Disabled Disabled
5 Disabled Disabled Disabled Disabled
6 Disabled Disabled Disabled Disabled
7 Disabled Disabled Disabled Disabled
8 Disabled Disabled Disabled Disabled
9 Disabled Disabled Disabled Disabled
10 Disabled Disabled Disabled Disabled
11 Disabled Disabled Disabled Disabled
12 Disabled Disabled Disabled Disabled
13 Disabled Disabled Disabled Disabled
14 Disabled Disabled Disabled Disabled
15 Disabled Disabled Disabled Disabled
16 Disabled Disabled Disabled Disabled
17 Disabled Disabled Disabled Disabled
18 Disabled Disabled Disabled Disabled
19 Disabled Disabled Disabled Disabled
20 Disabled Disabled Disabled Disabled
21 Disabled Disabled Disabled Disabled
22 Disabled Disabled Disabled Disabled
23 Disabled Disabled Disabled Disabled
24 Disabled Disabled Disabled Disabled
25 Disabled Disabled Disabled Disabled
26 Disabled Disabled Disabled Disabled
27 Disabled Disabled Disabled Disabled
28 Disabled Disabled Disabled Disabled

Figure 3 - 52. LLDP Basic TLVs Settings window

Use the drop-down menus to enable or disable the settings for the Basic TLVs Settings. Click **Apply** to implement changes made.

The following parameters can be set:

Parameter	Description
From Port/To Port	Use the pull-down menu to select a range of ports to be configured.
Port Description	Use the drop-down menu to enable or disable port description.
System Name	Use the drop-down menu to enable or disable system name.
System Description	Use the drop-down menu to enable or disable system description.
System Capabilities	Use the drop-down menu to enable or disable system capabilities.

Click **Apply** to implement changes made.

LLDP Dot1 TLVs Settings

LLDP Dot1 TLVs are organizationally specific TLVs which are defined in IEEE 802.1 and used to configure an individual port or group of ports to exclude one or more of the IEEE 802.1 organizational port vlan ID TLV data types from outbound LLDP advertisements.

To view this window, click **L2 Features > LLDP > LLDP Dot1 TLVs Settings**:

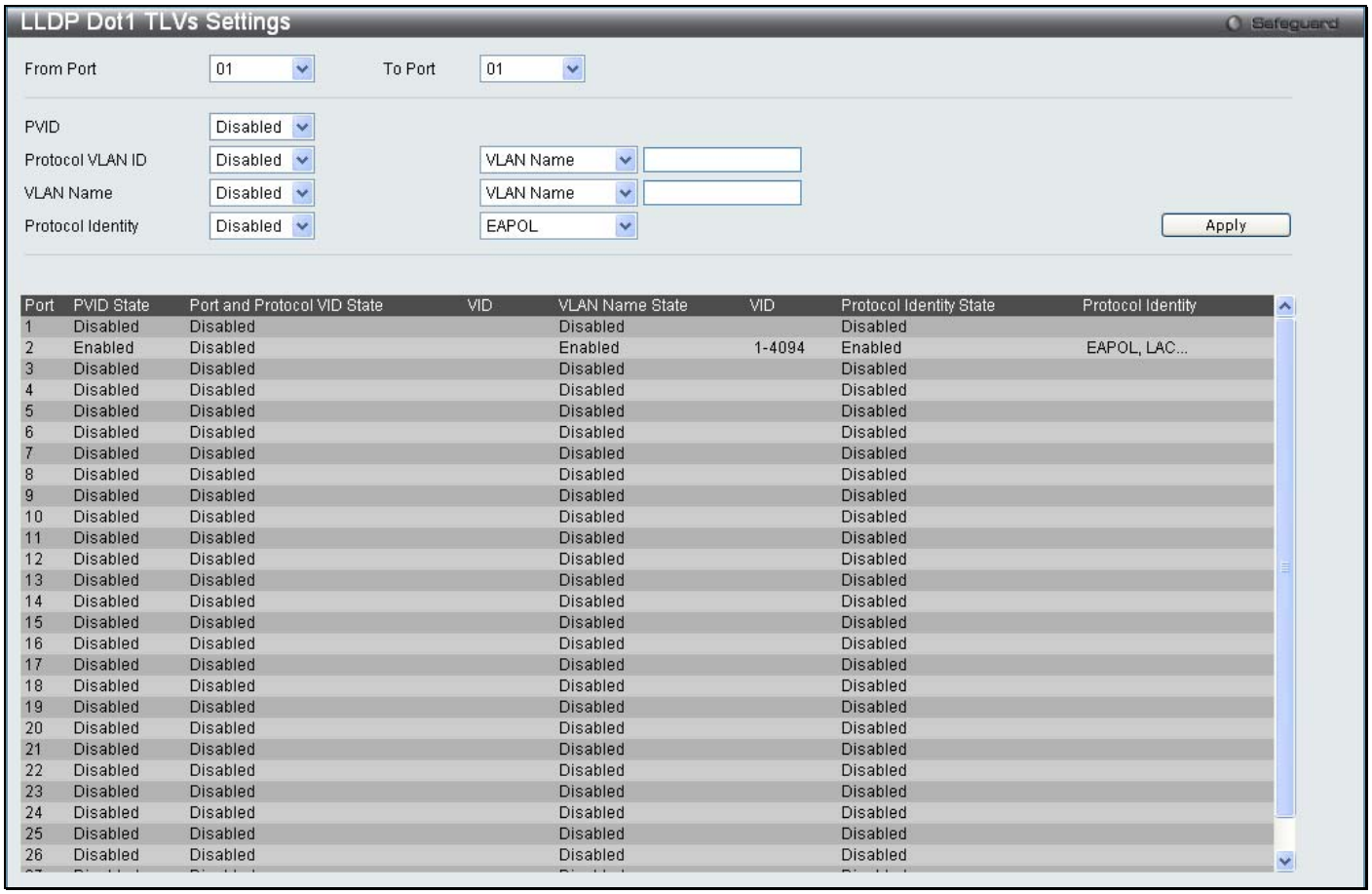

LLDP Dot1 TLVs Settings
Safeguard
From Port
01
To Port
01
PVID
Disabled
Protocol VLAN ID
Disabled
VLAN Name
VLAN Name
Disabled
VLAN Name
Protocol Identity
Disabled
EAPOL
Apply
Port PVID State Port and Protocol VID State VID VLAN Name State VID Protocol Identity State Protocol Identity
1 Disabled Disabled Disabled Disabled
2 Enabled Disabled Enabled 1-4094 Enabled EAPOL, LAC...
3 Disabled Disabled Disabled Disabled
4 Disabled Disabled Disabled Disabled
5 Disabled Disabled Disabled Disabled
6 Disabled Disabled Disabled Disabled
7 Disabled Disabled Disabled Disabled
8 Disabled Disabled Disabled Disabled
9 Disabled Disabled Disabled Disabled
10 Disabled Disabled Disabled Disabled
11 Disabled Disabled Disabled Disabled
12 Disabled Disabled Disabled Disabled
13 Disabled Disabled Disabled Disabled
14 Disabled Disabled Disabled Disabled
15 Disabled Disabled Disabled Disabled
16 Disabled Disabled Disabled Disabled
17 Disabled Disabled Disabled Disabled
18 Disabled Disabled Disabled Disabled
19 Disabled Disabled Disabled Disabled
20 Disabled Disabled Disabled Disabled
21 Disabled Disabled Disabled Disabled
22 Disabled Disabled Disabled Disabled
23 Disabled Disabled Disabled Disabled
24 Disabled Disabled Disabled Disabled
25 Disabled Disabled Disabled Disabled
26 Disabled Disabled Disabled Disabled

Figure 3 - 53. LLDP Dot1 TLVs Settings window

The following parameters can be set:

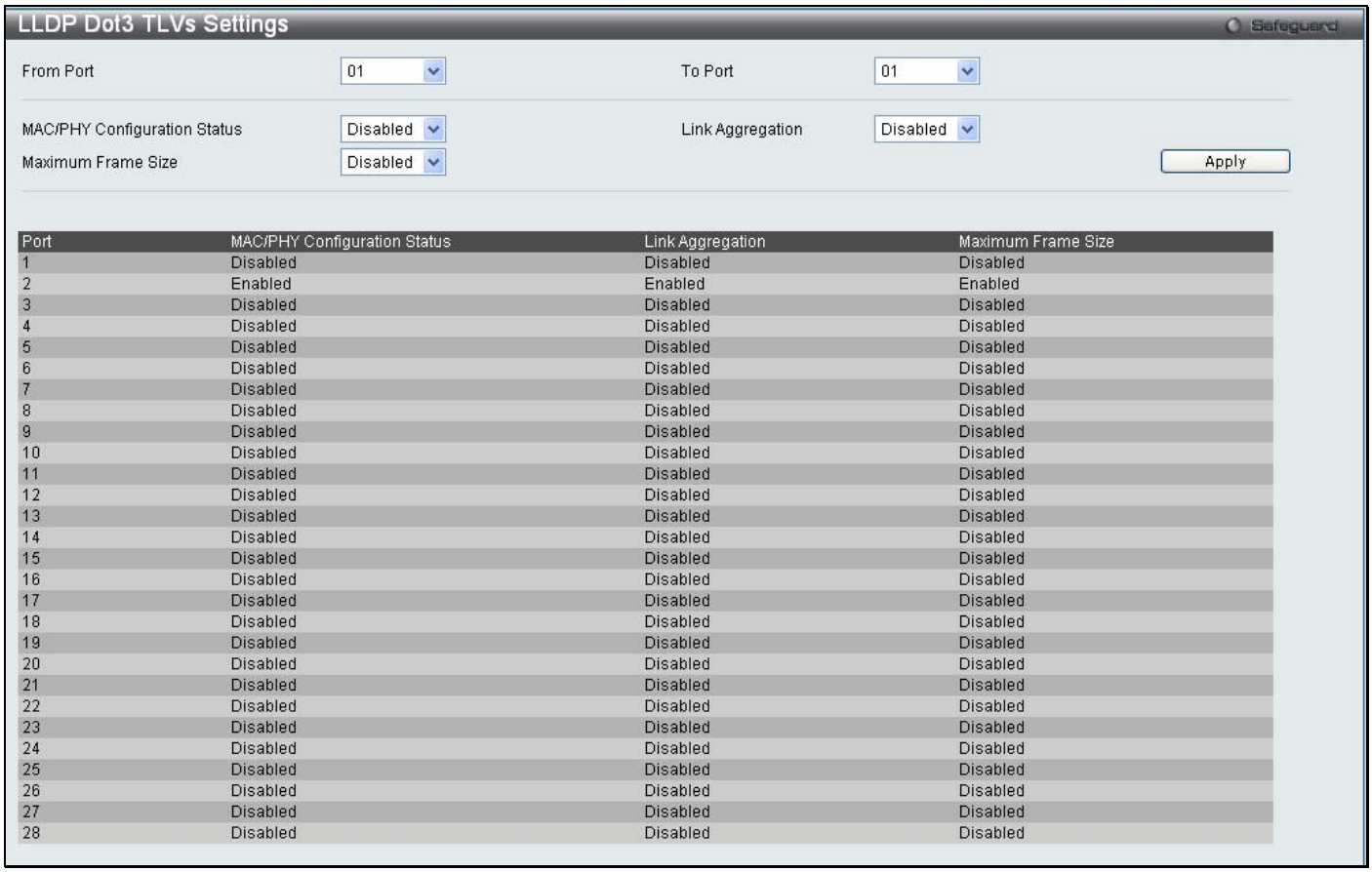
Parameter	Description
From Port/To Port	Use the pull-down menu to select a range of ports to be configured.
PVID	Use the drop-down menu to enable or disable the advertise PVID.
Protocol VLAN ID	Use the drop-down menu to enable or disable the advertise Protocol VLAN ID.
VLAN Name	Use the drop-down menu to enable or disable the advertise VLAN Name.
Protocol Identity	Use the drop-down menu to enable or disable the advertise Protocol Identity.

Click **Apply** to implement changes made.

LLDP Dot3 TLVs Settings

This window is used to configure an individual port or group of ports to exclude one or more IEEE 802.3 organizational specific TLV data type from outbound LLDP advertisements.

To view this window, click **L2 Features > LLDP > LLDP Dot3 TLVs Settings**:



Port	MAC/PHY Configuration Status	Link Aggregation	Maximum Frame Size
1	Disabled	Disabled	Disabled
2	Enabled	Enabled	Enabled
3	Disabled	Disabled	Disabled
4	Disabled	Disabled	Disabled
5	Disabled	Disabled	Disabled
6	Disabled	Disabled	Disabled
7	Disabled	Disabled	Disabled
8	Disabled	Disabled	Disabled
9	Disabled	Disabled	Disabled
10	Disabled	Disabled	Disabled
11	Disabled	Disabled	Disabled
12	Disabled	Disabled	Disabled
13	Disabled	Disabled	Disabled
14	Disabled	Disabled	Disabled
15	Disabled	Disabled	Disabled
16	Disabled	Disabled	Disabled
17	Disabled	Disabled	Disabled
18	Disabled	Disabled	Disabled
19	Disabled	Disabled	Disabled
20	Disabled	Disabled	Disabled
21	Disabled	Disabled	Disabled
22	Disabled	Disabled	Disabled
23	Disabled	Disabled	Disabled
24	Disabled	Disabled	Disabled
25	Disabled	Disabled	Disabled
26	Disabled	Disabled	Disabled
27	Disabled	Disabled	Disabled
28	Disabled	Disabled	Disabled

Figure 3 - 54. LLDP Dot3 TLVs Settings window

The following parameters can be set:

Parameter	Description
From Port / To Port	Use the drop-down menu to select a range of ports to be configured.
MAC/PHY Configuration Status	This TLV optional data type indicates that the LLDP agent should transmit 'MAC/PHY configuration/status TLV'. This indicates it is possible for two ends of an IEEE 802.3 link to be configured with different duplex and/or speed settings and still establish some limited network connectivity. More precisely, the information includes whether the port supports the auto-negotiation function, whether the function is enabled, whether it has auto-negotiated advertised capability, and what is the operational MAU type. The default state is *Disabled*.
Link Aggregation	The Link Aggregation option indicates that LLDP agents should transmit 'Link Aggregation TLV'. This indicates the current link aggregation status of IEEE 802.3 MACs. More precisely, the information should include whether the port is capable of doing link aggregation, whether the port is aggregated in an aggregated link, and what is the aggregated port ID. The default state is *Disabled*.
Maximum Frame Size	The Maximum Frame Size indicates that LLDP agent should transmit 'Maximum-frame-size TLV. The default state is *Disabled*.

Click **Apply** to implement changes made.

Section 4

QoS

Bandwidth Control

Traffic Control

802.1p Default Priority

802.1p User Priority

QoS Scheduling Settings

Priority Mapping

TOS Mapping

DSCP Map Settings

The Switch supports 802.1p priority queuing Quality of Service. The following section discusses the implementation of QoS (Quality of Service) and benefits of using 802.1p priority queuing.

Advantages of QoS

QoS is an implementation of the IEEE 802.1p standard that allows network administrators a method of reserving bandwidth for important functions that require a large amount of bandwidth or have a high priority, such as VoIP (Voice-over Internet Protocol), Web browsing applications, file server applications or video conferencing. Not only can larger bandwidth be created, but other less critical traffic can be limited, so excessive bandwidth can be saved. The Switch has separate hardware queues on every physical port to which packets from various applications can be mapped to, and, in turn prioritized. View the following map to see how the Switch implements 802.1P priority queuing.

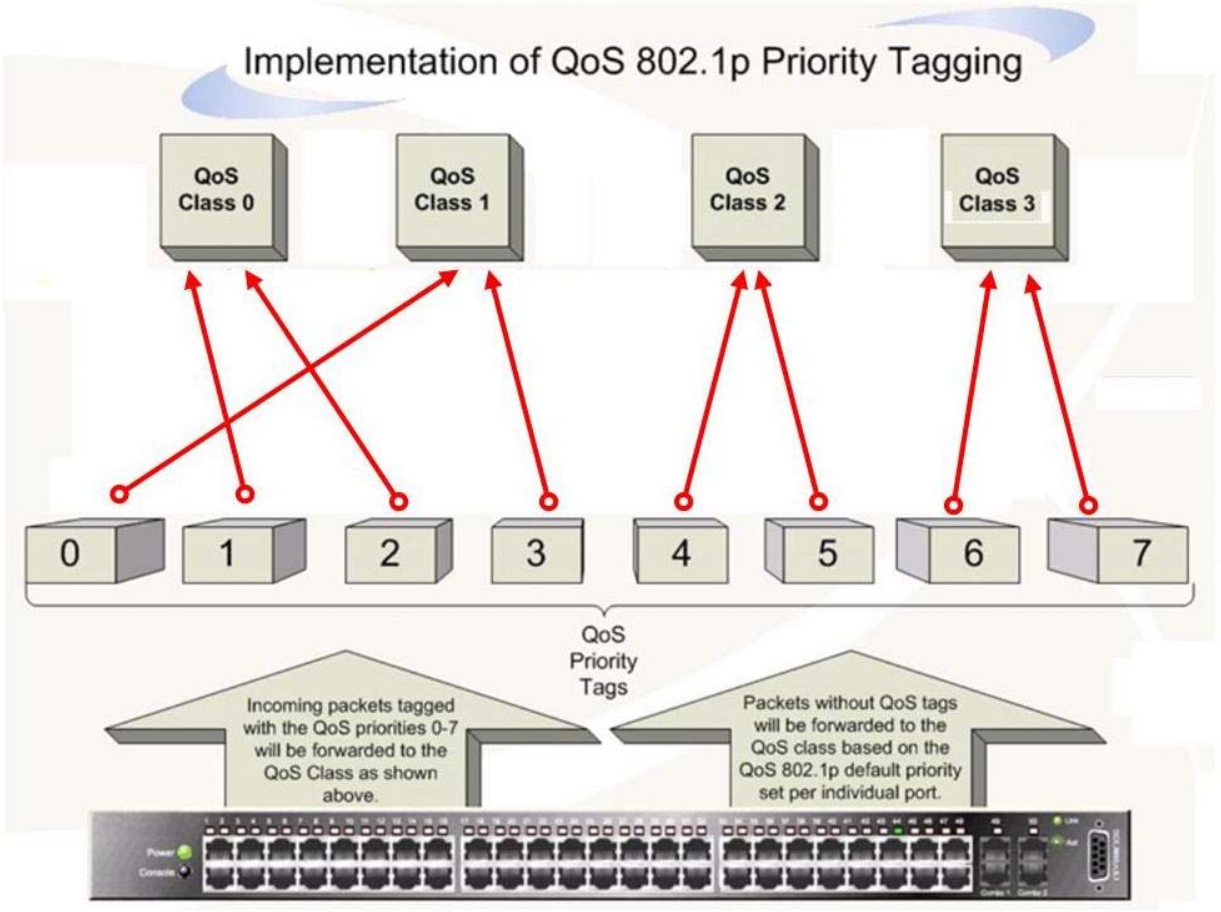

Implementation of QoS 802.1p Priority Tagging
QoS Class 0
QoS Class 1
QoS Class 2
QoS Class 3
0
1
2
3
4
5
6
7
QoS Priority Tags
Incoming packets tagged with the QoS priorities 0-7 will be forwarded to the QoS Class as shown above.
Packets without QoS tags will be forwarded to the QoS class based on the QoS 802.1p default priority set per individual port.

Figure 4 - 1. Mapping QoS on the Switch

The previous picture shows the default priority setting for the Switch. Class 3 has the highest priority of the four priority queues on the Switch. In order to implement QoS, the user is required to instruct the Switch to examine the header of a packet to see if it has the proper identifying tag tagged. Then the user may forward these tagged packets to designated queues on the Switch where they will be emptied, based on priority.

For example, if a user wishes to have a videoconference between two remotely set computers, the administrator can add priority tags to the video packets being sent out, utilizing the Access Profile commands. Then, on the receiving end, the administrator instructs the Switch to examine packets for this tag, acquires the tagged packets and maps them to a class queue on the Switch. Then in turn, the administrator will set a priority for this queue so that will be emptied before any other packet is forwarded. This result for the end user is receiving all packets sent as quickly as possible, thus prioritizing the queue and allowing for an uninterrupted stream of packets, which optimizes the use of bandwidth available for the video conference.

Understanding QoS

The Switch has four priority queues. These priority queues are labeled from 0 to 3, with 3 being the highest priority and 0 the lowest priority queue. The eight priority tags, specified in IEEE 802.1p are mapped to the Switch's priority tags as follows:

Priority 0 is assigned to the Switch's Q1 queue.

Priority 1 is assigned to the Switch's Q0 queue.

Priority 2 is assigned to the Switch's Q0 queue.

Priority 3 is assigned to the Switch's Q1 queue.

Priority 4 is assigned to the Switch's Q2 queue.

Priority 5 is assigned to the Switch's Q2 queue.

Priority 6 is assigned to the Switch's Q3 queue.

Priority 7 is assigned to the Switch's Q3 queue.

For strict priority-based scheduling, any packets residing in the higher priority queues are transmitted first. Multiple strict priority queues empty based on their priority tags. Only when these queues are empty, are packets of lower priority transmitted.

For weighted round robin queuing, the number of packets sent from each priority queue depends upon the assigned weight. For a configuration of four QoS queues, A~D with their respective weight value: 4~1, the packets are sent in the following sequence: A1, B1, C1, D1, A2, B2, C2, A3, B3, A4.

For weighted round robin queuing, if each QoS queue has the same weight value, then each QoS queue has an equal opportunity to send packets just like round robin queuing.

The Switch has four priority queues (and eight Classes of Service) for each port.

Bandwidth Control

The bandwidth control settings are used to place a ceiling on the transmitting and receiving data rates for any selected port.

To view this window, click **QoS > Bandwidth Control**:

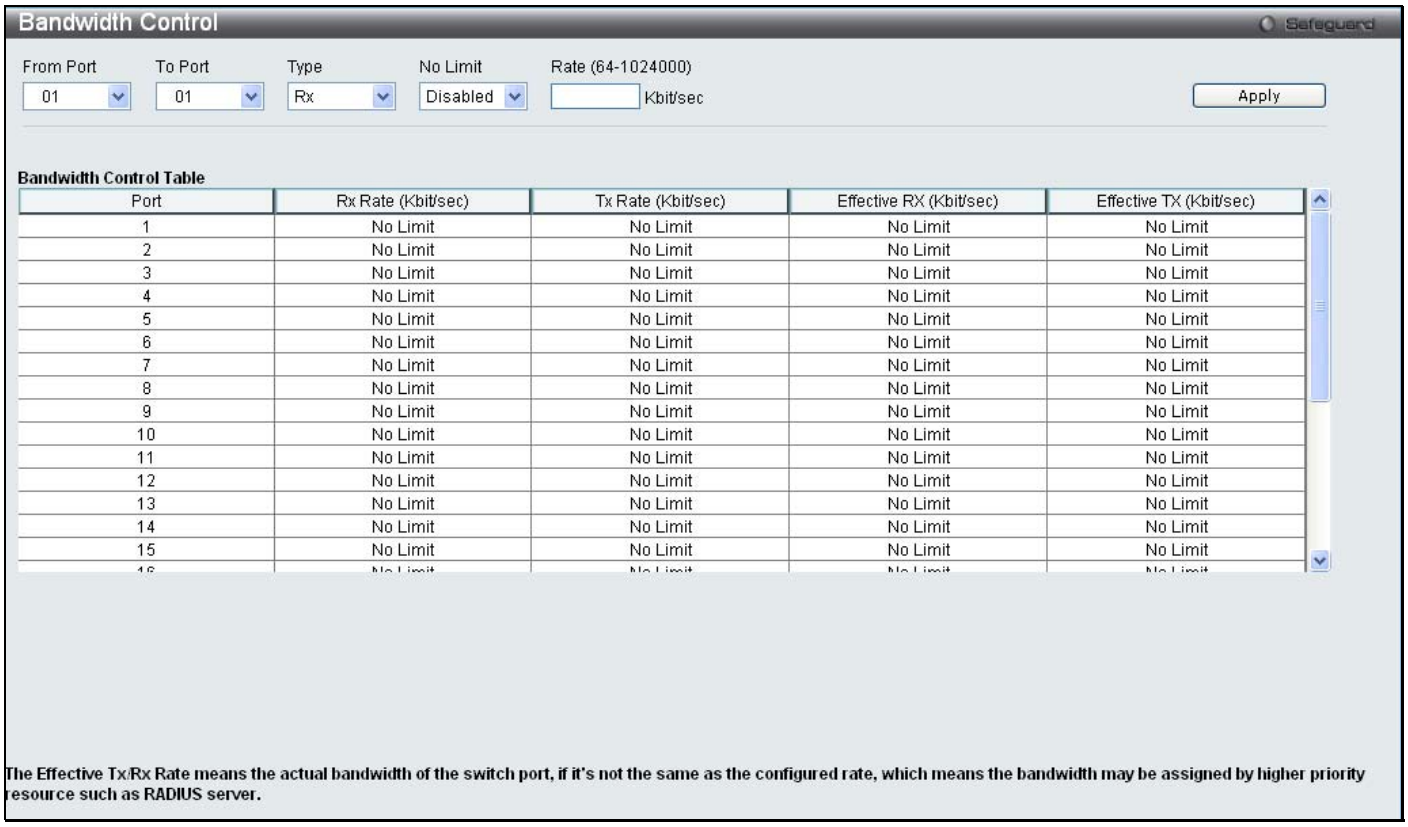

Bandwidth Control
Safeguard
From Port
01
To Port
01
Type
Rx
No Limit
Disabled
Rate (64-1024000)
Kbit/sec
Apply
Bandwidth Control Table
Port
Rx Rate (Kbit/sec)
Tx Rate (Kbit/sec)
Effective RX (Kbit/sec)
Effective TX (Kbit/sec)
1 No Limit No Limit No Limit No Limit
2 No Limit No Limit No Limit No Limit
3 No Limit No Limit No Limit No Limit
4 No Limit No Limit No Limit No Limit
5 No Limit No Limit No Limit No Limit
6 No Limit No Limit No Limit No Limit
7 No Limit No Limit No Limit No Limit
8 No Limit No Limit No Limit No Limit
9 No Limit No Limit No Limit No Limit
10 No Limit No Limit No Limit No Limit
11 No Limit No Limit No Limit No Limit
12 No Limit No Limit No Limit No Limit
13 No Limit No Limit No Limit No Limit
14 No Limit No Limit No Limit No Limit
15 No Limit No Limit No Limit No Limit
The Effective Tx/Rx Rate means the actual bandwidth of the switch port, if it's not the same as the configured rate, which means the bandwidth may be assigned by higher priority resource such as RADIUS server.

Figure 4 - 2. Bandwidth Control window

The following parameters can be set or are displayed:

Parameter	Description
From Port/To Port	A consecutive group of ports may be configured starting with the selected port.
Type	This drop-down menu allows you to select between *Rx* (receive), *Tx* (transmit), and *Both*. This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets.
No Limit	Use the drop-down menu to specify the selected port has limited or unlimited bandwidth.
Rate (64–1024000)	This field allows you to enter the data rate, in Kbits per second, that will be the limit for the selected port. The value must be a multiple of 64, between *64* and *1024000*.

Click **Apply** to set the bandwidth control for the selected ports. Results of configured Bandwidth Settings will be displayed in the **Bandwidth Control Table** on the lower half of the window.

Traffic Control

On a computer network, packets such as Multicast packets and Broadcast packets continually flood the network as normal procedure. At times, this traffic may increase due to a malicious endstation on the network or a malfunctioning device, such as a faulty network card. Thus, switch throughput problems will arise and consequently affect the overall performance of the switch network. To help rectify this packet storm, the Switch will monitor and control the situation.

The packet storm is monitored to determine if too many packets are flooding the network, based on the threshold level provided by the user. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided. This method can be utilized by selecting the Drop option of the Action field in the window below.

The Switch will also scan and monitor packets coming into the Switch by monitoring the Switch's chip counter. This method is only viable for Broadcast and Multicast storms because the chip only has counters for these two types of packets. Once a storm has been detected (that is, once the packet threshold set below has been exceeded), the Switch will shutdown the port to all incoming traffic with the exception of STP BPDU packets, for a time period specified using the CountDown field. If the packet storm discontinues before the Countdown timer expires, the port will again allow all incoming traffic. If this field times out and the packet storm continues, the port will be placed in a Shutdown Rest mode which will produce a warning message to be sent to the Trap Receiver. Once in Shutdown rEST mode, the port will be recovered after 5 minutes, or the user manually resets the port using the **Port Configuration** window in the **Configuration** folder and selecting the disabled port and returning it to an Enabled status. To utilize this method of Storm Control, choose the Shutdown option of the Action field in the window below.

To view this window, click **QoS > Traffic Control**:

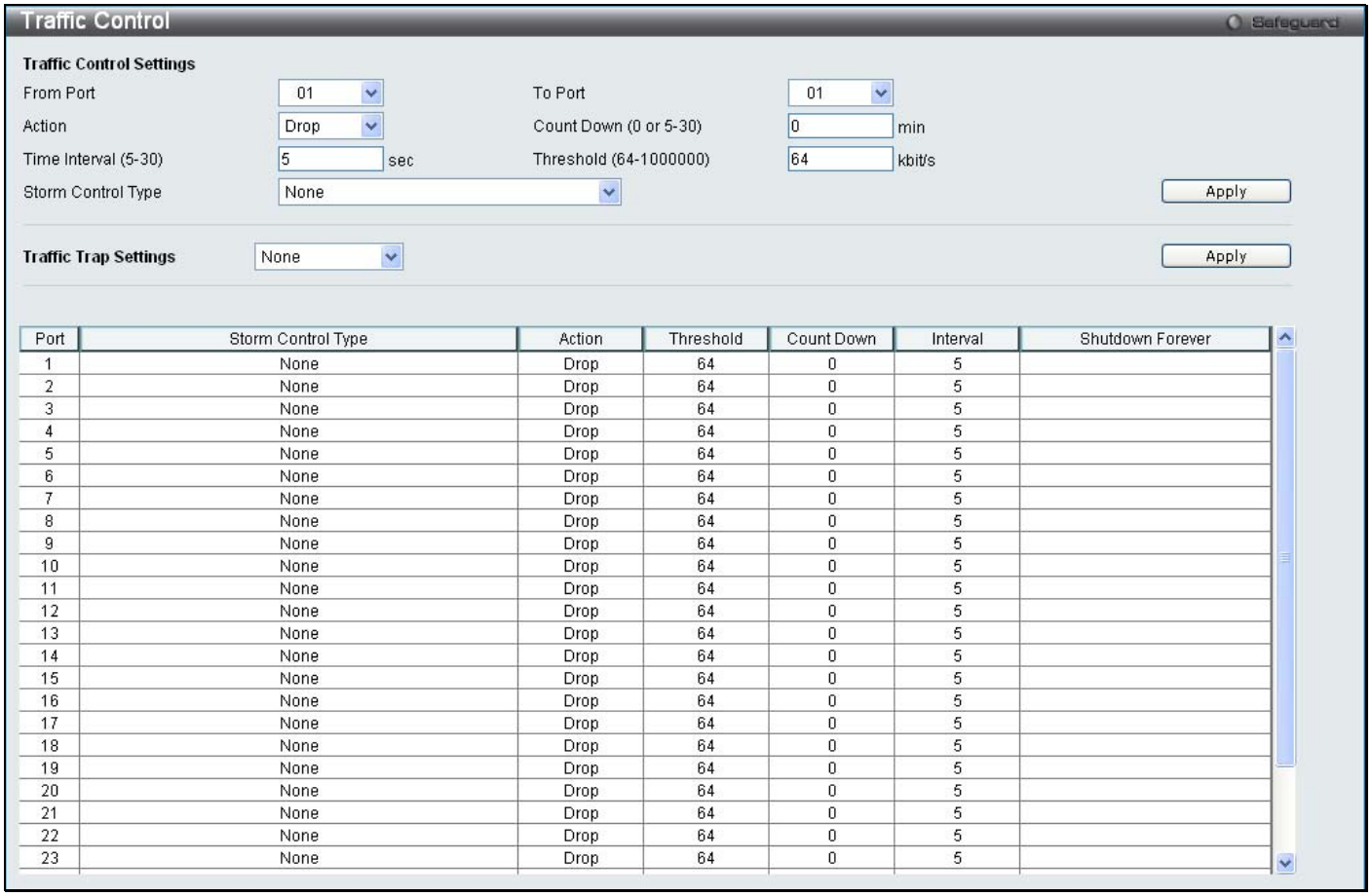

Traffic Control
Safeguard
Traffic Control Settings
From Port 01
To Port 01
Action Drop
Count Down (0 or 5-30) 0 min
Time Interval (5-30) 5 sec
Threshold (64-1000000) 64 kbit/s
Storm Control Type None
Apply
Traffic Trap Settings None
Apply
Port Storm Control Type Action Threshold Count Down Interval Shutdown Forever
1 None Drop 64 0 5
2 None Drop 64 0 5
3 None Drop 64 0 5
4 None Drop 64 0 5
5 None Drop 64 0 5
6 None Drop 64 0 5
7 None Drop 64 0 5
8 None Drop 64 0 5
9 None Drop 64 0 5
10 None Drop 64 0 5
11 None Drop 64 0 5
12 None Drop 64 0 5
13 None Drop 64 0 5
14 None Drop 64 0 5
15 None Drop 64 0 5
16 None Drop 64 0 5
17 None Drop 64 0 5
18 None Drop 64 0 5
19 None Drop 64 0 5
20 None Drop 64 0 5
21 None Drop 64 0 5
22 None Drop 64 0 5
23 None Drop 64 0 5

Figure 4 - 3. Traffic Control window

The following parameters can be set or are displayed:

Parameter	Description
Traffic Control Settings	
From Port/To Port	A consecutive group of ports may be configured starting with the selected port.

Action	Select the method of traffic Control from the pull-down menu. The choices are: *Drop* – Utilizes the hardware Traffic Control mechanism, which means the Switch's hardware will determine the Packet Storm based on the Threshold value stated and drop packets until the issue is resolved. *Shutdown* – Utilizes the Switch's software Traffic Control mechanism to determine the Packet Storm occurring. Once detected, the port will deny all incoming traffic to the port except STP BPDU packets, which are essential in keeping the Spanning Tree operational on the Switch. If the Countdown timer has expired and yet the Packet Storm continues, the port will be placed in Shutdown Rest mode. The port will be recovered after 5 minutes, or the user manually resets the port using the **Port Configuration** window in the **Configuration** folder and selecting the disabled port and returning it to an Enabled status. Choosing this option obligates the user to configure the Interval setting as well, which will provide packet count samplings from the Switch's chip to determine if a Packet Storm is occurring.
Count Down (0 or 5-30)	The Count Down timer is set to determine the amount of time, in minutes, that the Switch will wait before shutting down the port that is experiencing a traffic storm. Only the switch continues to experience a traffic storm during this countdown period and the switch will shutdown the port. This parameter is only useful for ports configured as Shutdown in their Action field and therefore will not operate for Hardware based Traffic Control implementations. The possible time settings for this field are *0*, *5* to *30* minutes. Zero means that the port will not enter shutdown rest mode.
Time Interval (5-30)	The Interval will set the time between Multicast and Broadcast packet counts sent from the Switch's chip to the Traffic Control function. These packet counts are the determining factor in deciding when incoming packets exceed the Threshold value. The Interval may be set between *5* and *30* seconds with the default setting of *5* seconds.
Threshold (64- 1000000)	Specifies the maximum number of packets per second that will trigger the Traffic Control function to commence. The configurable threshold range is from *64* to *1000000* with a default setting of *64*.
Storm Control Type	Select the type of Storm Type to detect: *Broadcast*, *Multicast*, *Unknown Unicast, Broadcast + Multicast*, *Broadcast + Unknown Unicast*, *Multicast + Unknown Unicast*, *Broadcast + Multicast + Unknown Unicast*, or *None*. Once selected, use the pull-down menu to enable or disable this storm detection.
Traffic Trap Setting	
Storm Trap	Enable sending of Storm Trap messages when the type of action taken by the Traffic Control function in handling a Traffic Storm is one of the following: • *None* – Will not send any Storm trap warning messages regardless of action taken by the Traffic Control mechanism. • *Storm Occurred* – Will send Storm Trap warning messages upon the occurrence of a Traffic Storm only. • *Storm Cleared* – Will send Storm Trap messages when a Traffic Storm has been cleared by the Switch only. • *Both* – Will send Storm Trap messages when a Traffic Storm has been both detected and cleared by the Switch. This function cannot be implemented in the Hardware mode. (When *Drop* is chosen in the Action field.

Click **Apply** to implement the settings made.

NOTE: Traffic Control cannot be implemented on ports that are set for Link Aggregation (Port Trunking).

NOTE: Ports that are in the Shutdown rest mode will be seen as Discarding in Spanning Tree windows and implementations though these ports will still be forwarding BPDUs to the Switch's CPU.

NOTE: Ports that are in Shutdown rest mode will be seen as link down in all windows and screens until the user recovers these ports.

802.1p Default Priority

The Switch allows the assignment of a default 802.1p priority to each port on the Switch.

To view this window, click **QoS > 802.1p Default Priority**:

802.1p Default Priority

Safeguard

From Port: 01 | To Port: 01 | Priority: 0 | Apply

Settings

Port	Priority	Effective Priority
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
16	0	0
17	0	0
18	0	0
19	0	0
20	0	0
21	0	0
22	0	0
23	0	0
24	0	0
25	0	0
26	0	0
27	0	0
28	0	0

Figure 4 - 4. 802.1p Default Priority window

This window allows assignment of a default 802.1p priority to any given port on the Switch. The priority values are numbered from 0, the lowest priority, to 7, the highest priority. Click **Apply** to implement the settings.

802.1p User Priority

The Switch allows the assignment of a user priority to each of the 802.1p priorities.

To view this window, click **QoS > 802.1p User Priority**:

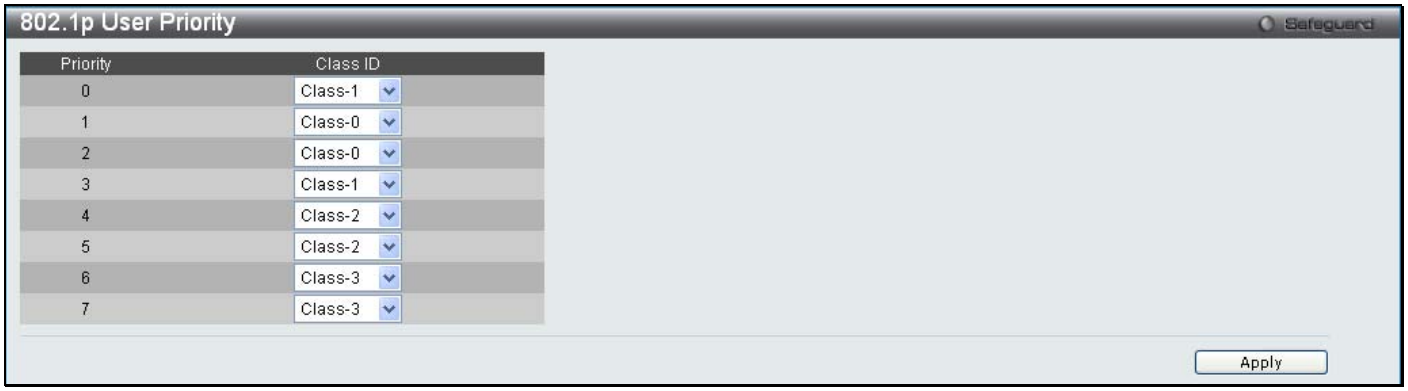


Figure 4 - 5. 802.1p User Priority window

Once a priority has been assigned to the port groups on the Switch, assign this Class to each of the eight levels of 802.1p priorities.

The following parameter may be set:

Parameter	Description
Class ID	This field is used to enter a Class ID between *Class-0* and *Class-3*.

Click **Apply** to set the changes.

QoS Scheduling Settings

Changing the output scheduling used for the hardware queues in the Switch can customize QoS. As with any changes to QoS implementation, careful consideration should be given to how network traffic in lower priority queues are affected. Changes in scheduling may result in unacceptable levels of packet loss or significant transmission delays. If you choose to customize this setting, it is important to monitor network performance, especially during peak demand, as bottlenecks can quickly develop if the QoS settings are not suitable.

To view this window, click **QoS > QoS Scheduling Settings**:

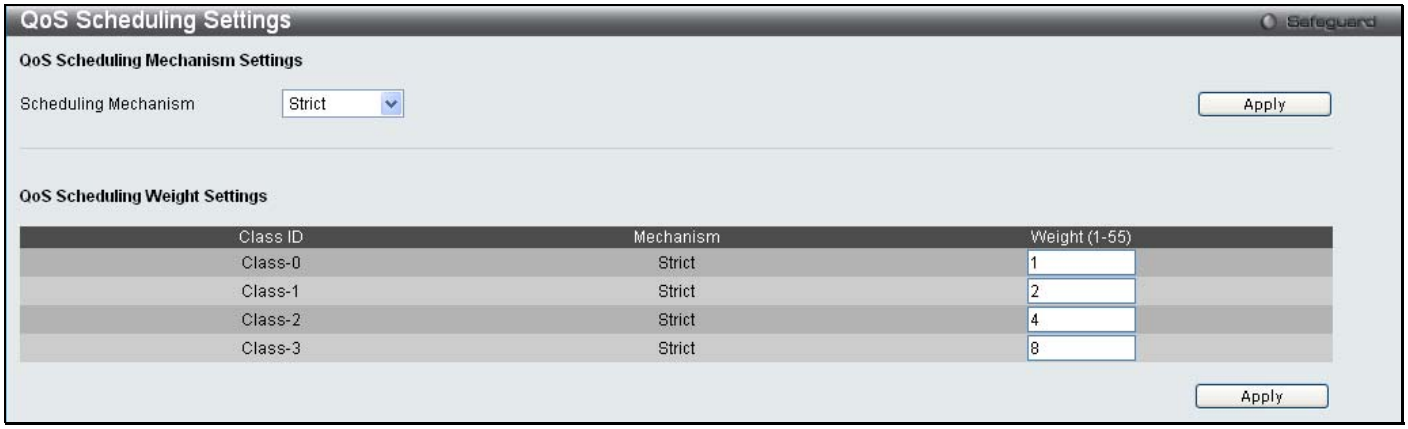


Figure 4 - 6. QoS Scheduling Settings window

The Scheduling Mechanism has the following parameters.

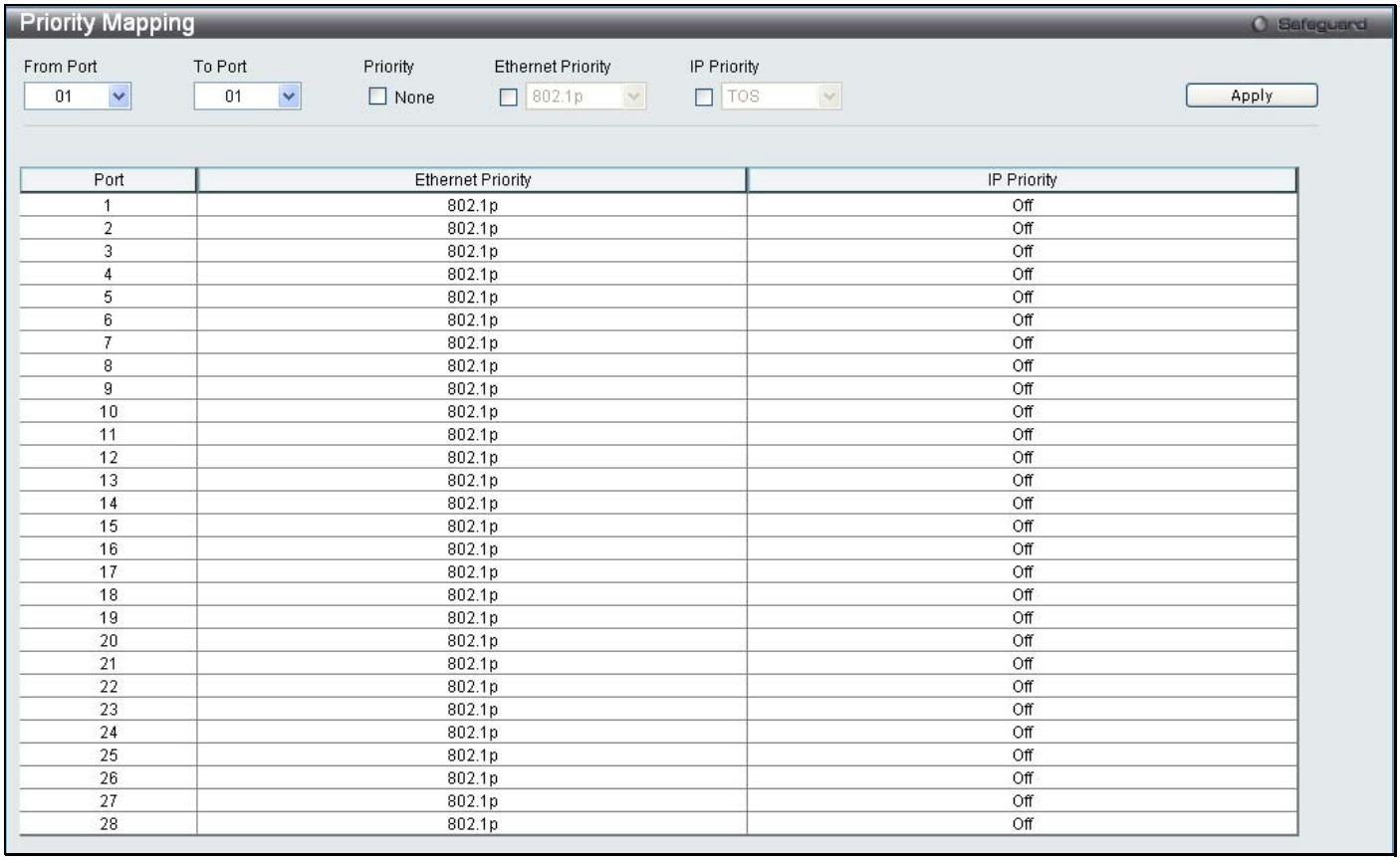
Parameter	Description
Scheduling Mechanism	Toggle between *Strict* and *Weight Fair*. *Strict* is the highest class of service and the first to process traffic. That is, the highest class of service will finish before other queues empty. *Weight Fair* uses the weighted round-robin algorithm to handle packets in an even distribution in priority classes of service.
Weight (1-55)	Enter a Weight value between *1* and *55*.

Click **Apply** to set the changes.

Priority Mapping

This window is used to set up Priority Mapping.

To view this window, click **QoS > Priority Mapping**:



Port	Ethernet Priority	IP Priority
1	802.1p	Off
2	802.1p	Off
3	802.1p	Off
4	802.1p	Off
5	802.1p	Off
6	802.1p	Off
7	802.1p	Off
8	802.1p	Off
9	802.1p	Off
10	802.1p	Off
11	802.1p	Off
12	802.1p	Off
13	802.1p	Off
14	802.1p	Off
15	802.1p	Off
16	802.1p	Off
17	802.1p	Off
18	802.1p	Off
19	802.1p	Off
20	802.1p	Off
21	802.1p	Off
22	802.1p	Off
23	802.1p	Off
24	802.1p	Off
25	802.1p	Off
26	802.1p	Off
27	802.1p	Off
28	802.1p	Off

Figure 4 - 7. Priority Mapping window

The following parameter may be set:

Parameter	Description
From Port/To Port	Select a range of ports to configure.
Priority	Tick the None check box neither Ethernet nor IP Priority mapping is desired.
Ethernet Priority	Tick the Ethernet Priority check box to set up 802.1p mapping.
IP Priority	Tick the IP Priority check box and then use the drop-down menu to select either *TOS* or *DSCP* mapping.

Click **Apply** to set the changes.

TOS Mapping

This window is used to set up Type of Service (TOS) Mapping.

To view this window, click **QoS > ToS Mapping**:

Figure 4 - 8. TOS Mapping window

The following parameter may be set:

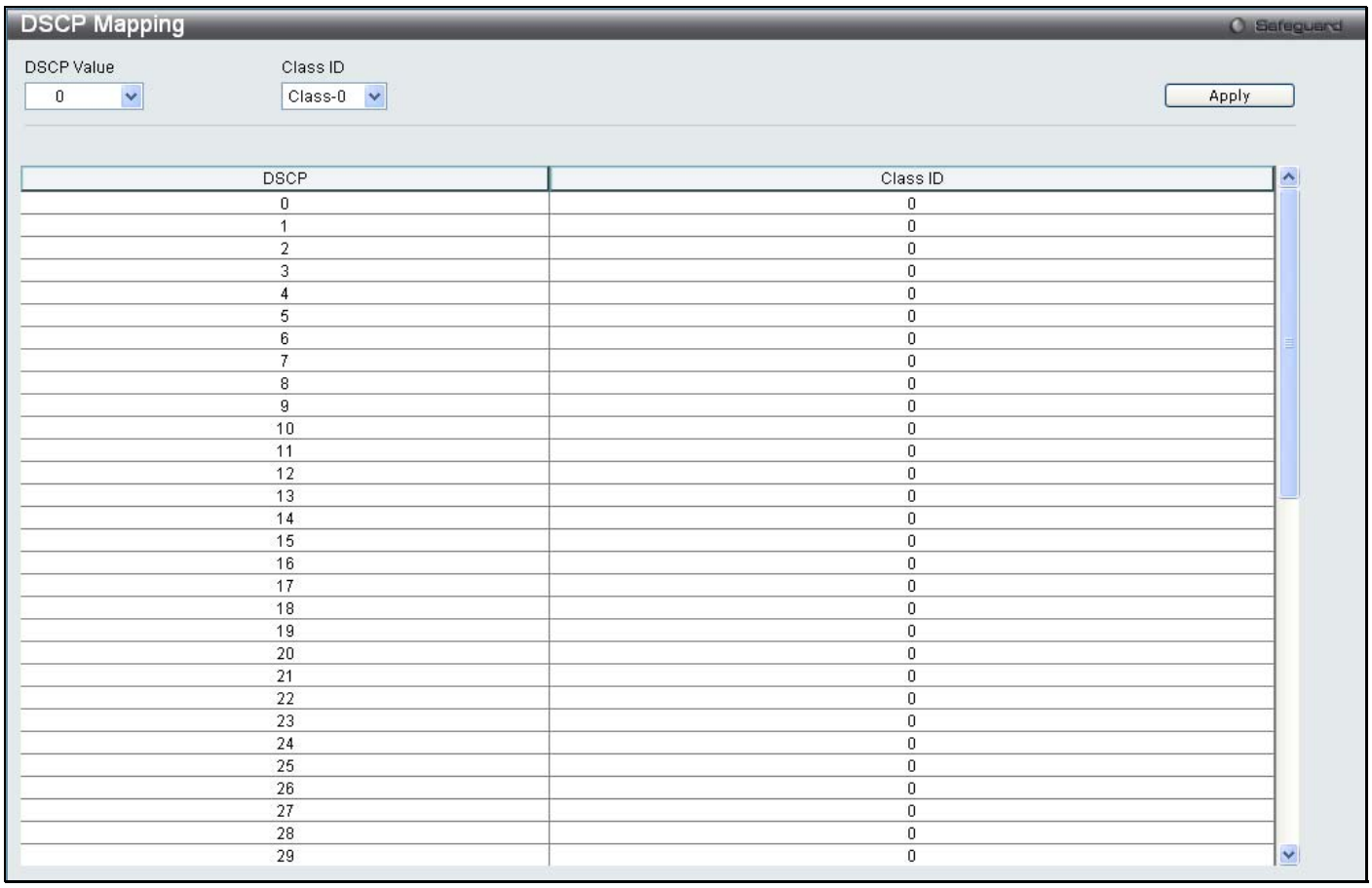
Parameter	Description
Class ID	This field is used to enter a Class ID between *Class-0* and *Class-3*.

Click **Apply** to set the changes.

DSCP Mapping

This window is used to set up DSCP Mapping.

To view this window, click **QoS > DSCP Mapping**:



DSCP	Class ID
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0
21	0
22	0
23	0
24	0
25	0
26	0
27	0
28	0
29	0

Figure 4 - 9. DSCP Mapping window

The following parameters may be set:

Parameter	Description
DSCP Value	This field is used to enter a DSCP value in the space provided, which will instruct the Switch to examine the DiffServ Code part of each packet header and use this as the main, or part of, the criterion for forwarding. The user may choose a value between *0* and *63*.
Class ID	This field is used to enter a Class ID between *Class-0* and *Class-3*.

Section 5

Security

Safeguard Engine

Trusted Host

IP-MAC-Port Binding

Port Security

DHCP Server Screening Settings

802.1X

SSL Settings

SSH

Access Authentication Control

MAC-based Access Control

DoS Prevention Settings

Safeguard Engine

Periodically, malicious hosts on the network will attack the Switch by utilizing packet flooding (ARP storm) or other methods. These attacks may affect normal traffic flow. To alleviate this problem, the Safeguard Engine function was added to the Switch's software.

The Safeguard Engine can help the overall operability of the Switch by minimizing the workload of the Switch during an attack, therefore making it capable of forwarding essential packets over the network with limited bandwidth. To achieve this, the Safeguard Engine uses threshold values to place the Switch in Exhausted or Normal mode.

The Switch will be placed in Exhausted mode when the CPU utilization exceeds the Rising Threshold. In Exhausted mode, the Switch will limit the bandwidth for ARP packets, therefore allowing more bandwidth for essential packets.

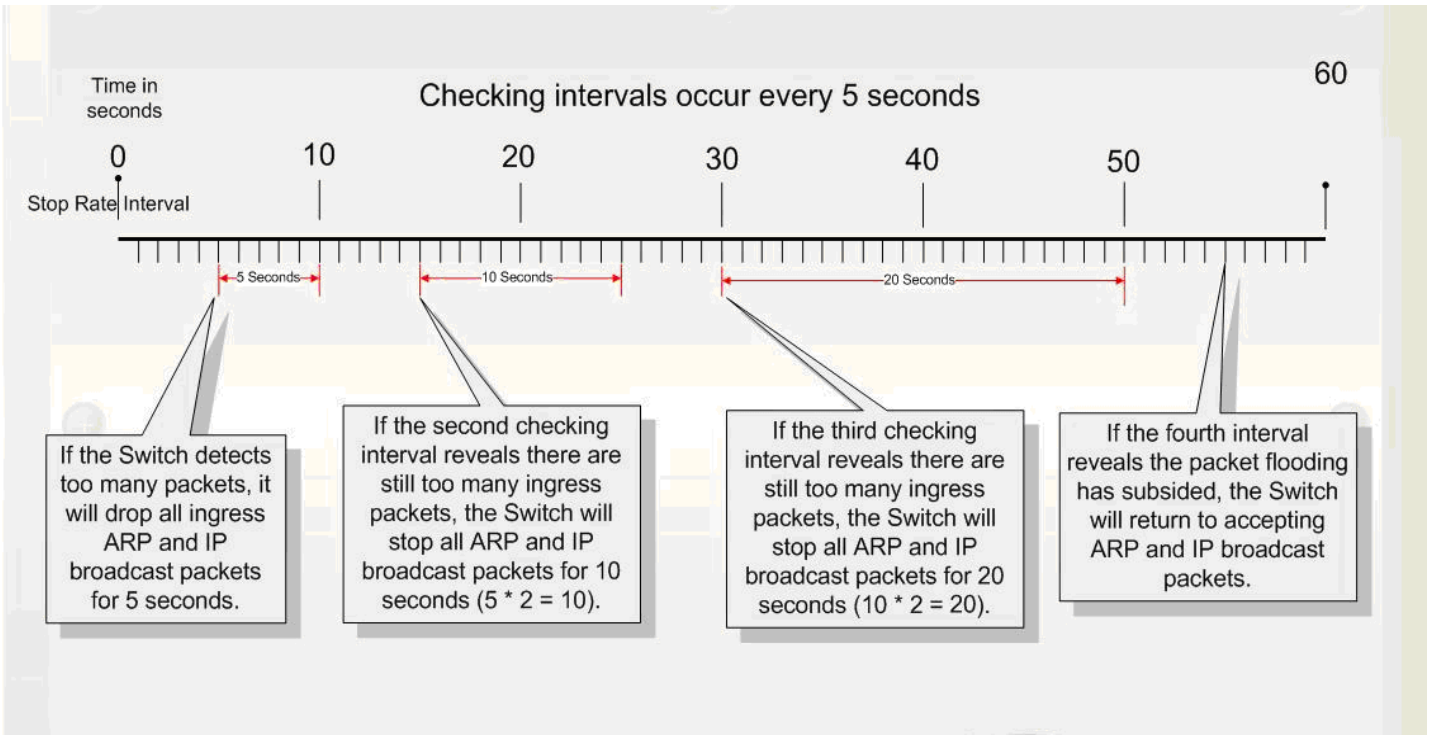

Time in seconds
Checking intervals occur every 5 seconds
60
0
10
20
30
40
50
Stop Rate Interval
5 Seconds
10 Seconds
20 Seconds
If the Switch detects too many packets, it will drop all ingress ARP and IP broadcast packets for 5 seconds.
If the second checking interval reveals there are still too many ingress packets, the Switch will stop all ARP and IP broadcast packets for 10 seconds (5 * 2 = 10).
If the third checking interval reveals there are still too many ingress packets, the Switch will stop all ARP and IP broadcast packets for 20 seconds (10 * 2 = 20).
If the fourth interval reveals the packet flooding has subsided, the Switch will return to accepting ARP and IP broadcast packets.

Figure 5 - 1. Safeguard Engine Checking Interval Example on the Switch

In Exhausted mode, two modes can be implemented to limit the bandwidth assigned to ARP packets, “Strict” and “Fuzzy”.

In Strict mode, the Switch will drop all ARP packets. The Switch will reluctantly process any packets not destined for the Switch and broadcast packets, no matter what is causing the high utilization rate on the CPU, which may not be an ARP storm.

In Fuzzy mode, the Switch uses an algorithm to assign different bandwidth levels for ARP packets. In Fuzzy mode, the Switch will analyze the rate of received ARP traffic to adjust the bandwidth dynamically. Once in Exhausted mode, the packet flow will decrease by half of the level that caused the Switch to enter Exhausted mode. After the packet flow has stabilized, the rate will initially increase by a small amount of processed packets and then return to a normal packet flow

In both Strict mode and Fuzzy mode the Safeguard Engine will check for packet flooding issues at regular intervals. For every consecutive checking interval that reveals a packet flooding issue, the Switch will double the time it will accept a few ingress ARP packets. In the example above, the Switch doubled the time for dropping ARP packets when consecutive flooding issues were detected at 5-second intervals. (First stop = 5 seconds, second stop = 10 seconds, third stop = 20 seconds) Once the flooding is no longer detected, the wait period for limiting ARP packets will return to 5 seconds and the process will resume.

To configure the Safeguard Engine for the Switch, click **Security > Safeguard Engine**, which will open the following window:

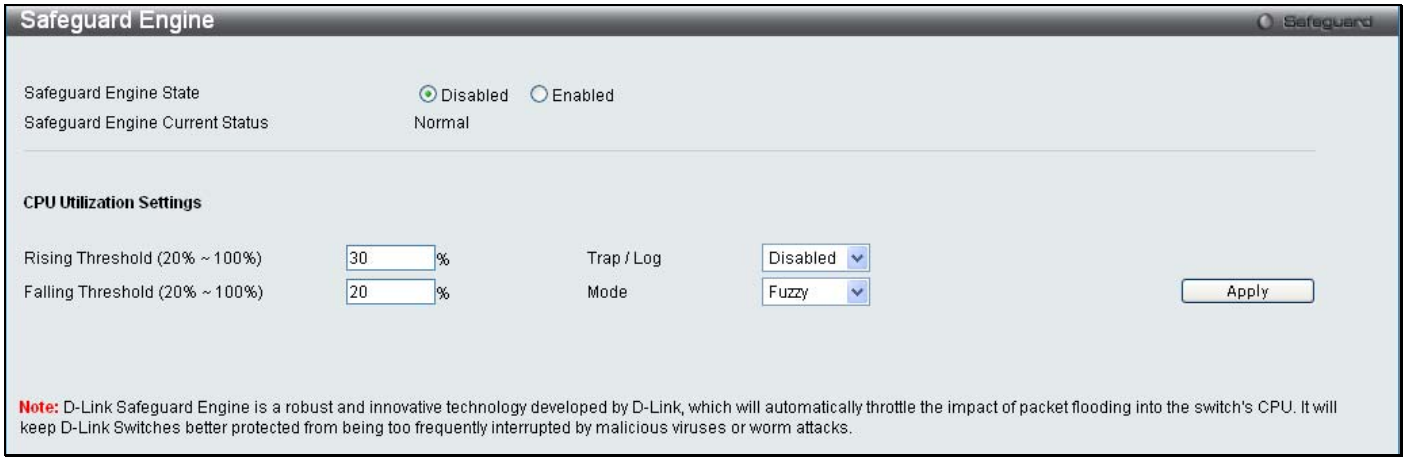

Safeguard Engine
Safeguard
Safeguard Engine State
Disabled
Enabled
Safeguard Engine Current Status
Normal
CPU Utilization Settings
Rising Threshold (20% ~ 100%)
30
%
Trap / Log
Disabled
Falling Threshold (20% ~ 100%)
20
%
Mode
Fuzzy
Apply
Note: D-Link Safeguard Engine is a robust and innovative technology developed by D-Link, which will automatically throttle the impact of packet flooding into the switch's CPU. It will keep D-Link Switches better protected from being too frequently interrupted by malicious viruses or worm attacks.

Figure 5 - 2. Safeguard Engine window

To configure the Switch’s Safeguard Engine, change the State to *Enabled* when the Safeguard Engine is enabled a green light will show on the gray bar at the top of this window, next to Safeguard. To set the Safeguard Engine for the Switch, complete the following fields:

Parameter	Description
Rising Threshold	Used to configure the acceptable level of CPU utilization before the Safeguard Engine mechanism is enabled. Once the CPU utilization reaches this percentage level, the Switch will move into the Exhausted state.
Falling Threshold	Used to configure the acceptable level of CPU utilization as a percentage, where the Switch leaves the Exhausted state and returns to normal mode.
Trap/log	Use the pull-down menu to enable or disable the sending of messages to the device’s SNMP agent and switch log once the Safeguard Engine has been activated by a high CPU utilization rate.
Mode	Toggle the State field to either *Strict* or *Fuzzy* for the Safeguard Engine of the Switch.

Click **Apply** to implement the settings made.

Trusted Host

Use the Security IP Management to permit remote stations to manage the Switch. If one or more designated management stations are defined by the user, only the chosen stations, as defined by IP address, will be allowed management privilege through the Web manager, Telnet session, or SNMP manager. To define a management station IP setting, type in the IP address with a proper subnet mask and click the **Add** button.

To view this window, click **Security > Trusted Host**:

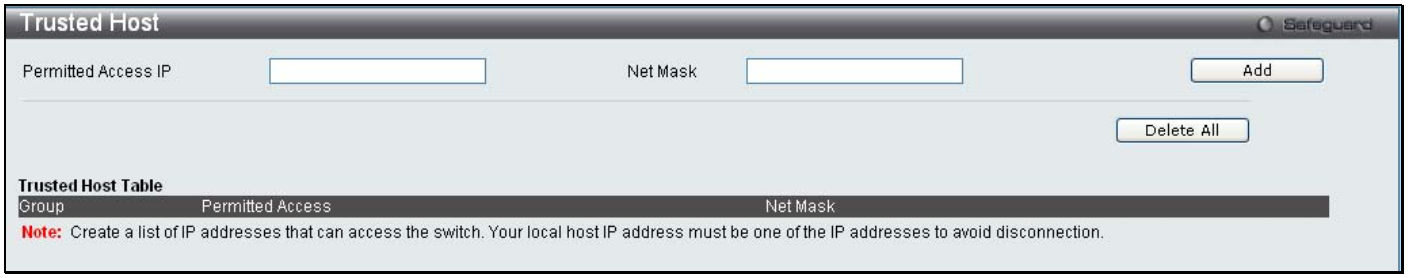

Trusted Host
Safeguard
Permitted Access IP
Net Mask
Add
Delete All
Trusted Host Table
Group
Permitted Access
Net Mask
Note: Create a list of IP addresses that can access the switch. Your local host IP address must be one of the IP addresses to avoid disconnection.

Figure 5 - 3. Trusted Host window

To delete an entry, click the corresponding **Delete** button. To delete all the entries on the Trusted Host Table, click the **Delete All** button.

IP-MAC-Port Binding

The IP network layer uses a four-byte address. The Ethernet link layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC-port binding is to restrict access to the Switch to a number of authorized users. Only authorized clients can access the Switch's port by checking the pair of IP-MAC addresses with the pre-configured database. If an unauthorized user tries to access an IP-MAC-port binding enabled port, the system will block the access by dropping its packet. The maximum number of IP-MAC-port binding entries is dependant on chip capability (e.g. the ARP table size) and storage size of the device. Active and inactive entries use the same database. The maximum entry number is 500. The creation of authorized users can be manually configured by CLI or Web. The function is port-based, meaning a user can enable or disable the function on the individual port.

IMP Binding Global Settings

This window is used to enable or disable the Trap Log State and DHCP Snoop state on the Switch. The Trap/Log field will enable and disable the sending of trap log messages for IP-MAC-port binding. When enabled, the Switch will send a trap message to the SNMP agent and the Switch log when an ARP packet is received that doesn't match the IP-MAC-port binding configuration set on the Switch.

To view this window click, **Security > IP-MAC-Port Binding > IMP Binding Global Settings**:

Figure 5 - 4. IMP Binding Global Settings window

The following parameters can be set:

Parameter	Description
Trap / Log	This field will enable and disable the sending of trap log messages for IP-MAC-port binding. When *Enabled*, the Switch will send a trap log message to the SNMP agent and the Switch log when an ARP packet is received that doesn't match the IP-MAC-port binding configuration set on the Switch.

DHCP Snoop State	Use the pull-down menu to enable or disable the DHCP Snooping State for IP-MAC-port binding.
ARP Inspection	When this is *Enabled*, the Switch will filter ARP packets which have unauthorized sender MACs, IP addresses, and ingress ports. ARP inspection is only active on IP-MAC-port binding-enabled ports.
Recover Learning Ports (e.g.: 1, 7-12)	Enter the ports for which the ARP check function has stopped. This will allow recovery, or an unfreezing, of the ARP check on the ports listed in this field. Alternatively, tick All to force the recovery of all learning ports.

Click **Apply** to implement the settings made.

IMP Binding Port Settings

Select a port or a range of ports with the From Port and To Port fields. Enable or disable the port with the State, Allow Zero IP, Forward DHCP Packet, Mode, and SLT fields, and configure the port's Max Entry value.

To view this window click, **Security > IP-MAC-Port Binding > IMP Binding Port Settings**:

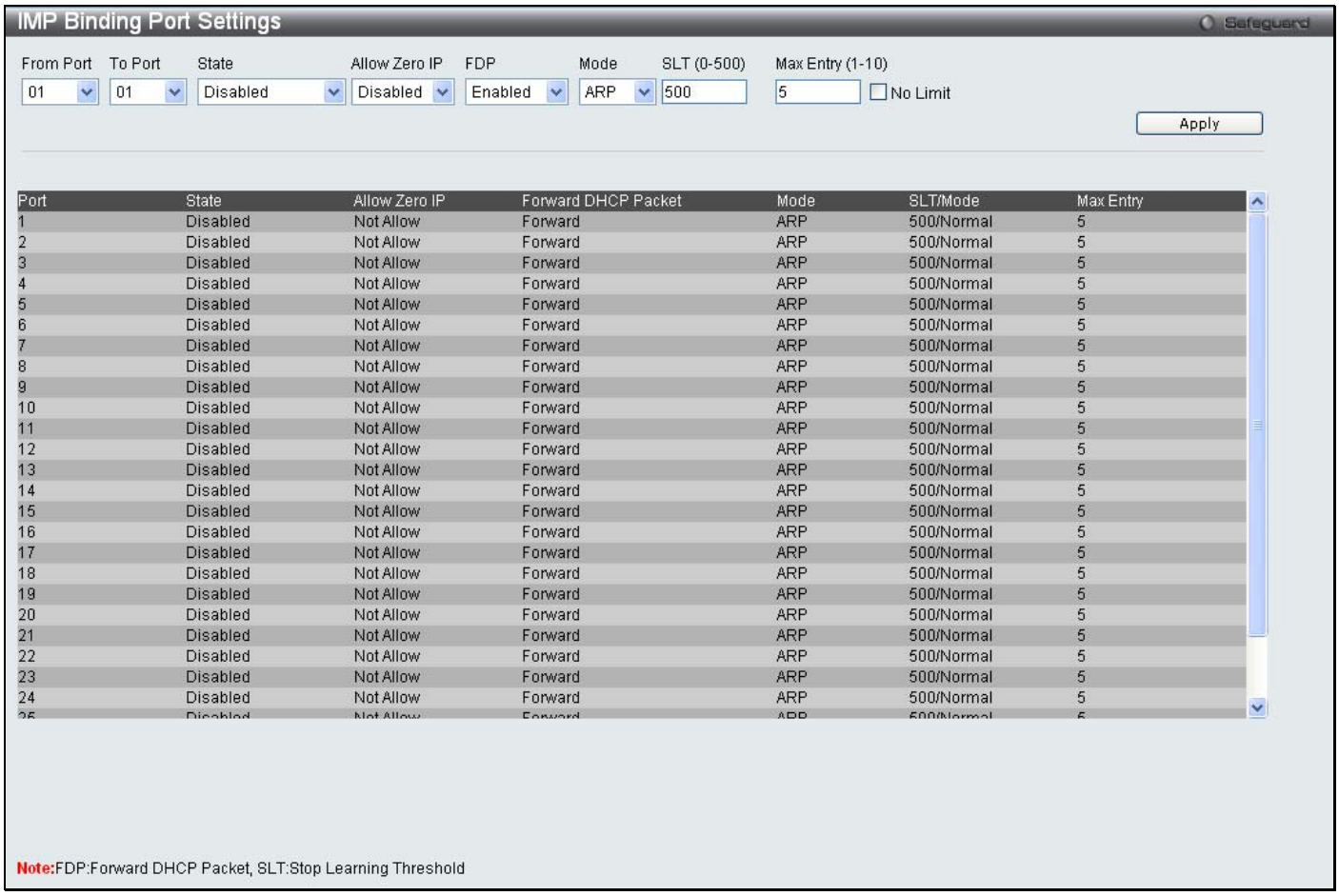


Figure 5 - 5. IMP Binding Port Settings window

The following fields can be set or modified:

Parameter	Description
From Port/To Port	Select a port or range of ports to set for IP-MAC Binding.
State	Use the pull-down menu to Enable or Disable these ports for IP-MAC Binding. *Enabled (Strict)* – This mode provides a stricter method of control. If the user selects this mode, all packets will be sent to the CPU, thus all packets will not be forwarded by the

	hardware until the S/W learns the entries for the ports. The port will check ARP packets and IP packets by IP-MAC-port binding entries. When the packet is found by the entry, the MAC address will be set to dynamic. If the packet is not found by the entry, the MAC address will be set to block. Other packets will be dropped. The default mode is *Enabled (Strict)* if not specified. *Enabled (Loose)* – This mode provides a looser way of control. If the user selects loose mode, ARP packets and IP Broadcast packets will be sent to the CPU. The packets will still be forwarded by the hardware until a specific source MAC address is blocked by the software. The port will check ARP packets and IP Broadcast packets by IP-MAC-port binding entries. When the packet is found by the entry, the MAC address will be set to dynamic. If the packet is not found by the entry, the MAC address will be set to block. Other packets will be bypassed.
Allow Zero IP	Use the drop-down menu to enable or disable this feature. Zero IP configures the state which allows ARP packets with 0.0.0.0 source IP to bypass.
FDP	By default, the DHCP packet with broadcast DA will be flooded. When set to *Disabled*, the broadcast DHCP packet received by the specified port will not be forwarded.
Mode	The user may set the mode for this IP-MAC-port binding settings by choosing *ARP* or *ACL*. When configuring the mode of the port to *ACL*, the Switch will create an ACL access entry corresponding to the entries of this port. If the port changes to *ARP*, all the ACL entries will be deleted automatically. The default mode is *ARP*.
SLT (0-500)	Enter a Stop-learning Threshold value between *0* and *500*. The default SLT for each port is *500*.
Max Entry (1-50)	Specifies the maximum number of IP-MAC-port binding entries between *1* and *50*. The default is *5*. Alternatively, tick the No Limit check box.

IMP Binding Entry Settings

This window is used to create static IP- MAC-port binding entries on the Switch.

To view this window click, **Security > IP-MAC-Port Binding > IMP Binding Entry Settings**:

Figure 5 - 6. IMP Binding Entry Settings window

The following fields can be set or modified:

Parameter	Description
IP Address	Enter the IP address to bind to the MAC address set below.
MAC Address	Enter the MAC address to bind to the IP Address set above.
Ports	Specify the Switch ports for which to configure this IP-MAC-port binding entry (IP Address + MAC Address). Tick the All Ports check box to configure this entry for all ports on the Switch.

Click **Apply** for implement changes, click **Find** to search for an entry, click **Show All** for the table to display all entries and click **Delete** to remove an entry.

DHCP Snooping Entries

This window is used to view dynamic entries on specific ports. To view particular port settings, enter the port number and click **Find**. To view all entries click **View All**, and to delete an entry, click **Clear**.

To view this window click, **Security > IP-MAC-Port Binding > DHCP Snooping Entries**:

Figure 5 - 7. DHCP Snooping Entries window

MAC Block List

This window is used to view unauthorized devices that have been blocked by IP-MAC binding restrictions. To find an unauthorized device that has been blocked by the IP-MAC binding restrictions, enter the VID and MAC Address in the appropriate fields and click **Find**. To delete an entry, click the delete button next to the entry's port. To display all the MAC blocked entries, click **View All**.To delete all the entries in the window, click **Delete All**.

To view this window click, **Security > IP-MAC-Port Binding > MAC Block List**:

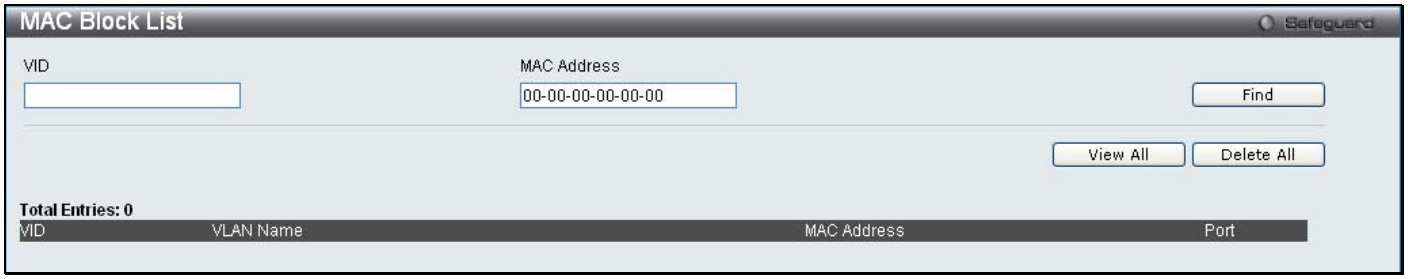


Figure 5 - 8. MAC Block List window

Port Security

Port Security is a security feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch prior to locking the port (or ports) from connecting to the Switch's locked ports and gaining access to the network.

Port Security Port Settings

A given ports' (or a range of ports') dynamic MAC address learning can be locked such that the current source MAC addresses entered into the MAC address forwarding table can not be changed once the port lock is enabled. Setting the Admin State pull-down menu to *Enabled*, and clicking **Apply** can lock the port.

To view the following window, click, **Security > Port Security > Port Security Port Settings**:

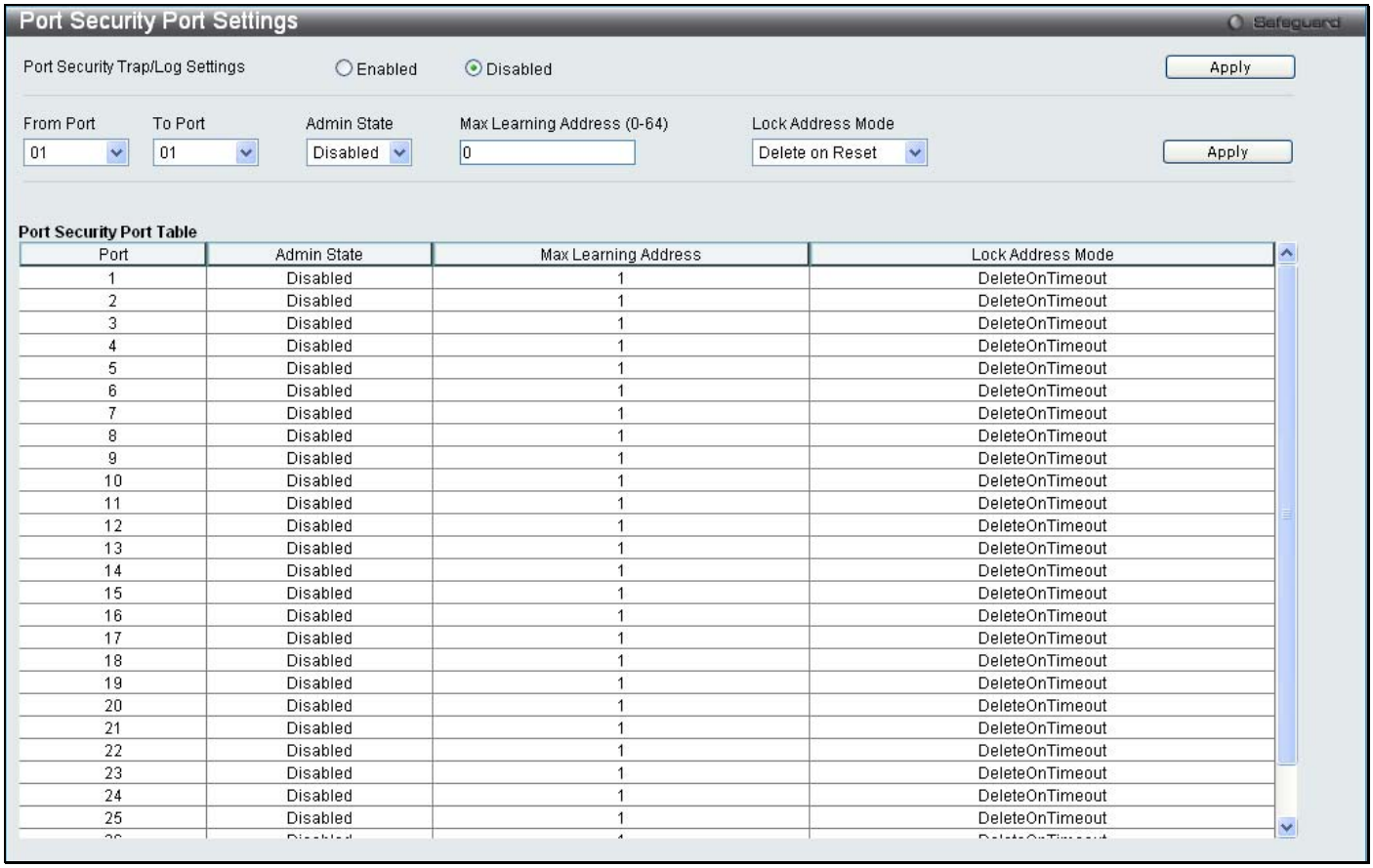


Figure 5 - 9. Port Security Port Settings window

The following parameters can be set:

Parameter	Description
From Port/To Port	A consecutive group of ports may be configured starting with the selected port.
Admin State	This pull-down menu allows you to enable or disable Port Security (locked MAC address table for the selected ports).
Max. Learning Address (0-64)	The number of MAC addresses that will be in the MAC address-forwarding table for the selected switch and group of ports.
Lock Address Mode	This pull-down menu allows you to select how the MAC address table locking will be implemented on the Switch, for the selected group of ports. The options are: *Permanent* – The locked addresses will not age out after the aging timer expires. *Delete on Timeout* – The locked addresses will age out after the aging timer expires. *Delete on Reset* – The locked addresses will not age out until the Switch has been reset.

Click **Apply** to implement changes made.

Port Security FDB Entries

This window is used to clear the Port Lock Entries by individual ports. To clear entries enter the range of ports and click **Clear**.

To view the following window click, **Security > Port Security > Port Security FDB Entries**:

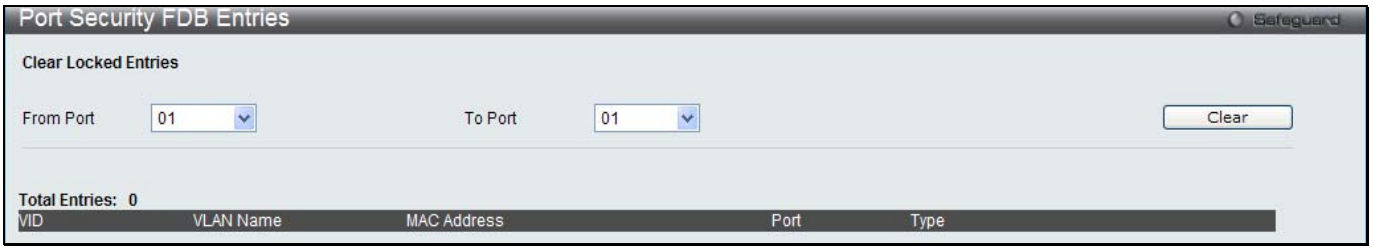


Figure 5 - 10. Port Security FDB Entries window

802.1X

The IEEE 802.1X standard is a security measure for authorizing and authenticating users to gain access to various wired or wireless devices on a specified Local Area Network by using a Client and Server based access control model. This is accomplished by using a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the Client and the Server. The following figure represents a basic EAPOL packet:

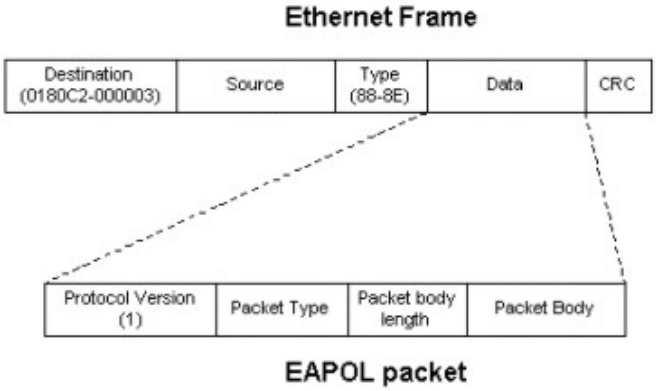


Figure 5 - 11. The EAPOL Packet

Utilizing this method, unauthorized devices are restricted from connecting to a LAN through a port to which the user is connected. EAPOL packets are the only traffic that can be transmitted through the specific port until authorization is granted. The 802.1X Access Control method holds three roles, each of which are vital to creating and upkeeping a stable and working Access Control security method.

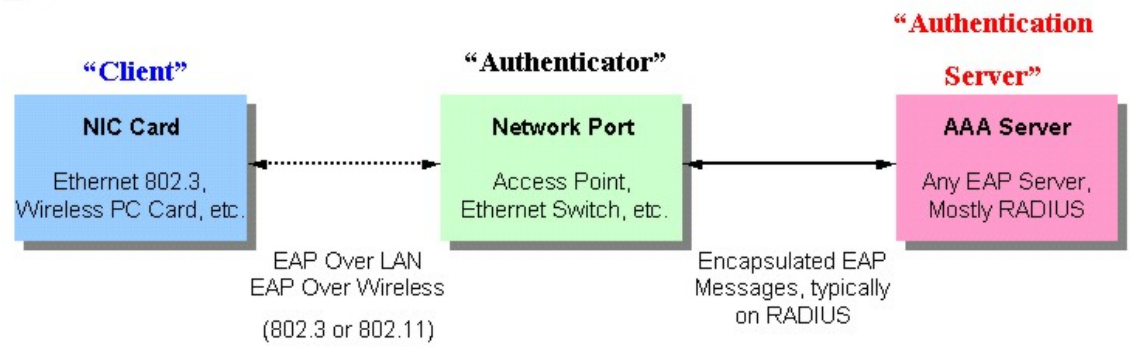


Figure 5 - 12. The three roles of 802.1X

The following section will explain the three roles of Client, Authenticator and Authentication Server in greater detail.

Authentication Server

The Authentication Server is a remote device that is connected to the same network as the Client and Authenticator, must be running a RADIUS Server program and must be configured properly on the Authenticator (Switch). Clients connected to a port on the Switch must be authenticated by the Authentication Server (RADIUS) before attaining any services offered by the Switch on the LAN. The role of the Authentication Server is to certify the identity of the Client attempting to access the network by exchanging secure information between the RADIUS server and the Client through EAPOL packets and, in turn, informs the Switch whether or not the Client is granted access to the LAN and/or switches services.

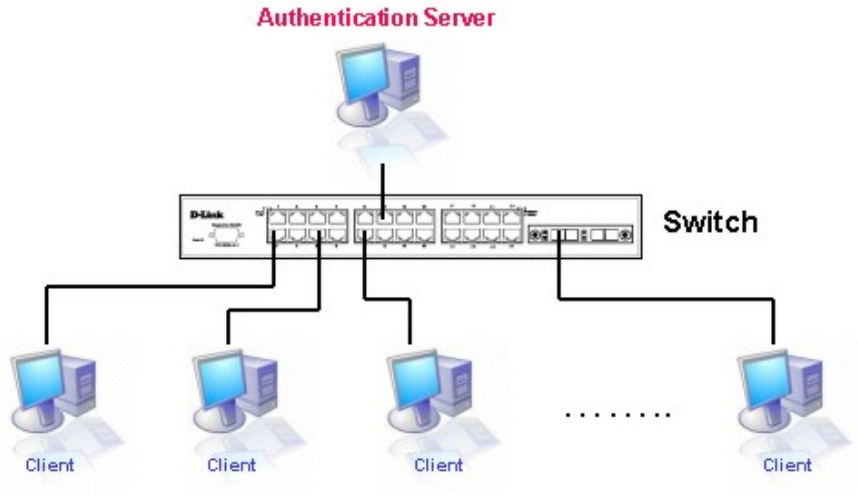


Figure 5 - 13. The Authentication Server

Authenticator

The Authenticator (the Switch) is an intermediary between the Authentication Server and the Client. The Authenticator serves two purposes when utilizing the 802.1X function. The first purpose is to request certification information from the Client through EAPOL packets, which is the only information allowed to pass through the Authenticator before access is granted to the Client. The second purpose of the Authenticator is to verify the information gathered from the Client with the Authentication Server, and to then relay that information back to the Client.

Three steps must be implemented on the Switch to properly configure the Authenticator.

1. The 802.1X state must be *Enabled*. (**Security / 802.1X /802.1X Settings**)
2. The 802.1X settings must be implemented by port (**Security** / **802.1X** / **802.1X Settings**)
3. A RADIUS server must be configured on the Switch. (**Security** / **802.1X** / **Authentic RADIUS Server**)

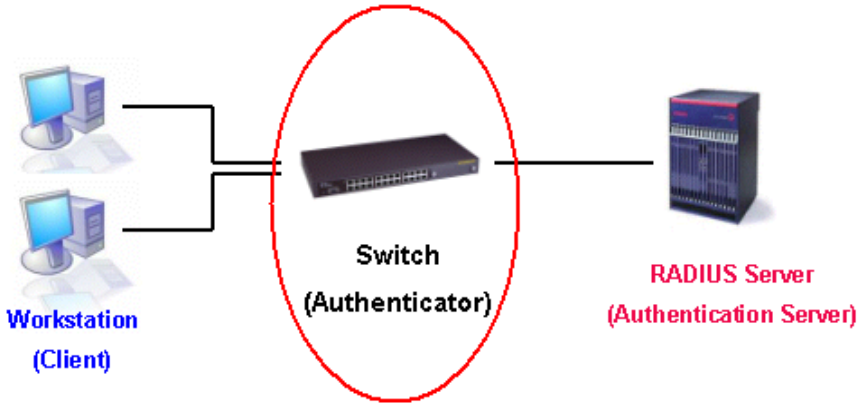


Figure 5 - 14. The Authenticator

NOTE: When configuring the Authentication Protocol as local, the Switch has two roles: Authenticator and Authentication Server.

Client

The Client is simply the endstation that wishes to gain access to the LAN or switch services. All endstations must be running software that is compliant with the 802.1X protocol. For users running Windows XP, that software is included within the operating system. All other users are required to attain 802.1X client software from an outside source. The Client will request access to the LAN and or Switch through EAPOL packets and, in turn will respond to requests from the Switch.

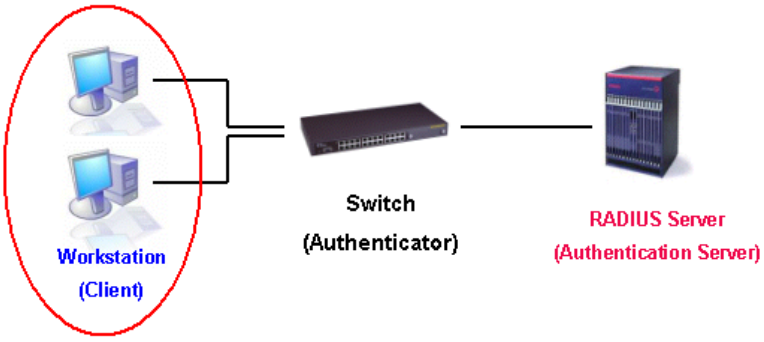


Figure 5 - 15. The Client

Authentication Process

Utilizing the three roles stated above, the 802.1X protocol provides a stable and secure way of authorizing and authenticating users attempting to access the network. Only EAPOL traffic is allowed to pass through the specified port before a successful authentication is made. This port is “locked” until the point when a Client with the correct username and password (and MAC address if 802.1X is enabled by MAC address) is granted access and therefore successfully “unlocks” the port. Once the port is unlocked, normal traffic is allowed to pass through the port. The following figure displays a more detailed explanation of how the authentication process is completed between the three roles stated above.

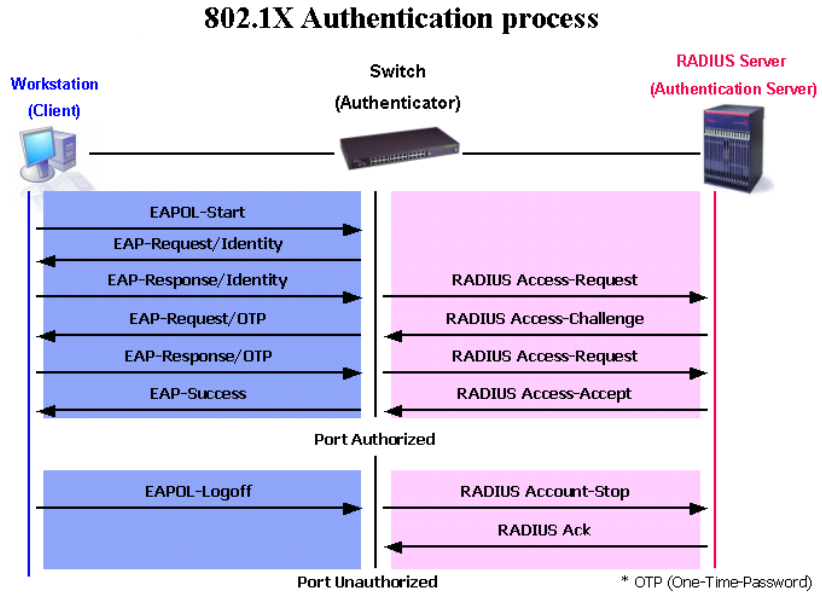


Figure 5 - 16. The 802.1X Authentication Process

The D-Link implementation of 802.1X allows network administrators to choose between two types of Access Control used on the Switch, which are:

1. Port-Based Access Control – This method requires only one user to be authenticated per port by a remote RADIUS server to allow the remaining users on the same port access to the network.
2. MAC-Based Access Control – Using this method, the Switch will automatically learn up to 448 MAC addresses by port and set them in a list. Each MAC address must be authenticated by the Switch using a remote RADIUS server before being allowed access to the Network.

Understanding 802.1X Port-based and MAC-based Network Access Control

The original intent behind the development of 802.1X was to leverage the characteristics of point-to-point in LANs. As any single LAN segment in such infrastructures has no more than two devices attached to it, one of which is a Bridge Port. The Bridge Port detects events that indicate the attachment of an active device at the remote end of the link, or an active device becoming inactive. These events can be used to control the authorization state of the Port and initiate the process of authenticating the attached device if the Port is unauthorized. This is the Port-Based Network Access Control.

Port-Based Network Access Control

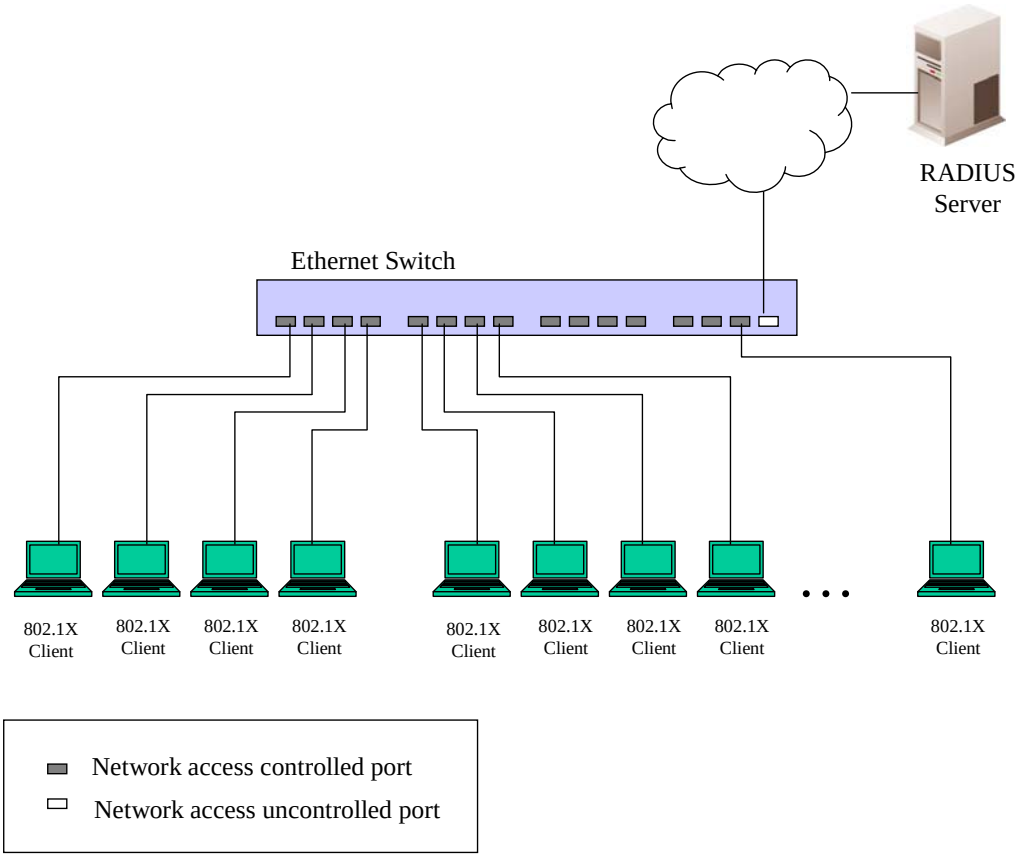


Figure 5 - 17. Example of Typical Port-Based Configuration

Once the connected device has successfully been authenticated, the Port then becomes Authorized, and all subsequent traffic on the Port is not subject to access control restriction until an event occurs that causes the Port to become Unauthorized. Hence, if the Port is actually connected to a shared media LAN segment with more than one attached device, successfully authenticating one of the attached devices effectively provides access to the LAN for all devices on the shared segment. Clearly, the security offered in this situation is open to attack.

MAC-Based Network Access Control

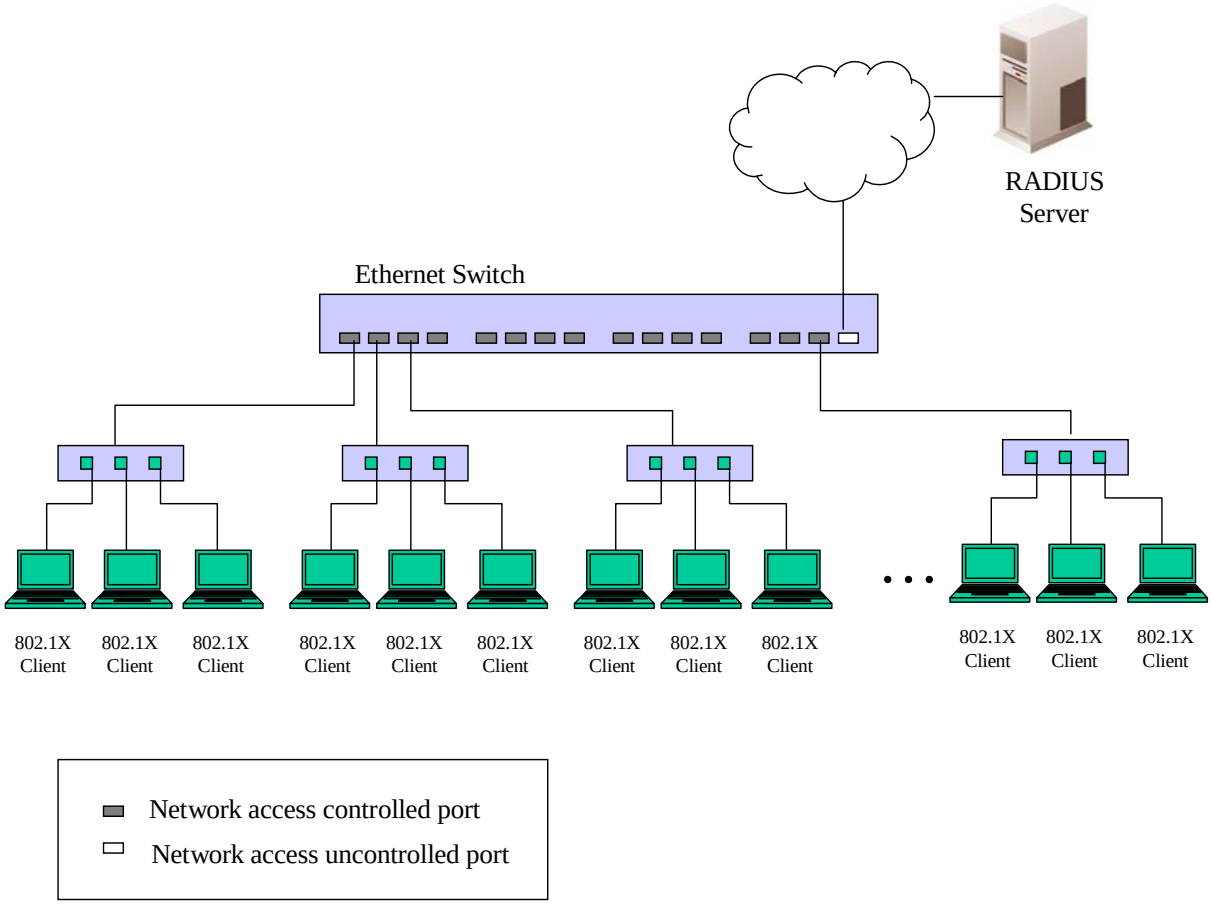


Figure 5 - 18. Example of Typical MAC-Based Configuration

In order to successfully make use of 802.1X in a shared media LAN segment, it would be necessary to create “logical” Ports, one for each attached device that required access to the LAN. The Switch would regard the single physical Port connecting it to the shared media segment as consisting of a number of distinct logical Ports, each logical Port being independently controlled from the point of view of EAPOL exchanges and authorization state. The Switch learns each attached devices’ individual MAC addresses, and effectively creates a logical Port that the attached device can then use to communicate with the LAN via the Switch.

802.1X Settings

To configure the 802.1X Settings, click **Security > 802.1X > 802.1X Settings**:

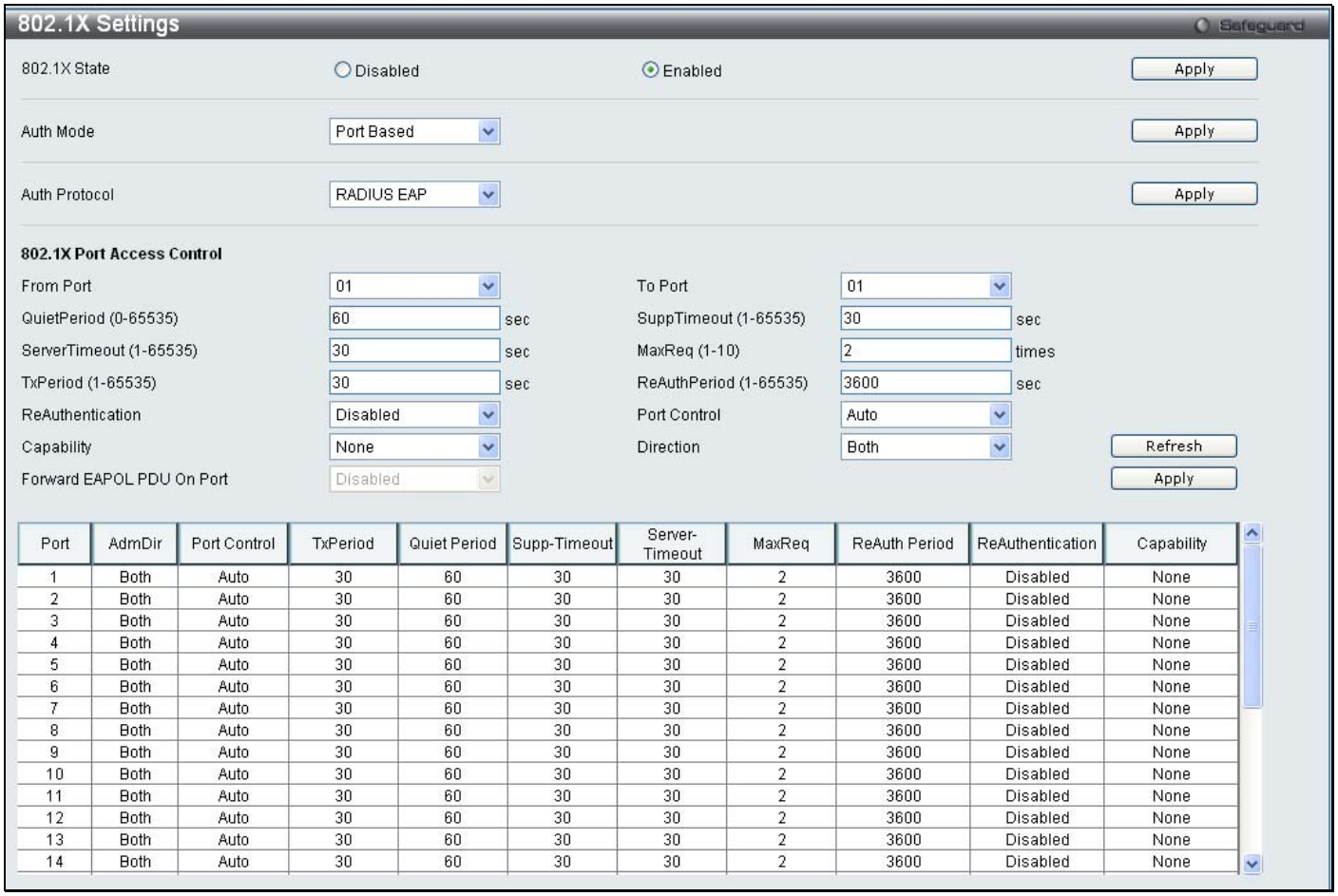


Figure 5 - 19. 802.1X Settings window

This window allows you to set the following features:

Parameter	Description
802.1X	Use the radio buttons to enable or disable 802.1X.
Auth Mode	Choose the 802.1X authentication mode, *Port Based*, or *MAC Based*.
Auth Protocol	Choose the authentication protocol, *Local* or *RADIUS EAP.*
From Port/To Port	Enter the port or ports to be set.
QuietPeriod (0-65535)	This allows you to set the number of seconds that the Switch remains in the quiet state following a failed authentication exchange with the client. The default setting is *60* seconds.
SuppTimeout (1-65535)	This value determines timeout conditions in the exchanges between the Authenticator and the client. The default setting is *30* seconds.
ServerTimeout (1-65535)	This value determines timeout conditions in the exchanges between the Authenticator and the authentication server. The default setting is *30* seconds.
MaxReq (1-10)	The maximum number of times that the Switch will retransmit an EAP Request to the client before it times out of the authentication sessions. The default setting is *2*.
TxPeriod	This sets the TxPeriod of time for the authenticator PAE state machine. This value determines

(1-65535)	the period of an EAP Request/Identity packet transmitted to the client. The default setting is *30* seconds.
ReAuthPeriod (1-65535)	A constant that defines a nonzero number of seconds between periodic reauthentication of the client. The default setting is *3600* seconds.
ReAuthentication	Determines whether regular reauthentication will take place on this port. The default setting is *Disabled*.
Port Control	This allows you to control the port authorization state. Select *ForceAuthorized* to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client. If *ForceUnauthorized* is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface. If *Auto* is selected, it will enable 802.1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server. The default setting is *Auto*.
Capability	This allows the 802.1X Authenticator settings to be applied on a per-port basis. Select *Authenticator* to apply the settings to the port. When the setting is activated A user must pass the authentication process to gain access to the network. Select *None* disable 802.1X functions on the port.
Direction	Sets the administrative-controlled direction to either *in* or *both*. If *In* is selected, control is only exerted over incoming traffic through the port you selected in the first field. If *Both* are selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field.
Forward EAPOL PDU On Port	This enables or disables the Switch retransmit EAPOL PDU Request on a per port basis.

Click **Apply** to implement your configuration changes.

802.1X User

To create a new 802.1X User enter a user name and password then reconfirm the password and click **Apply**, the new user will be displayed in the lower half of the table. To delete an entry click the corresponding **Delete** button.

To configure the 802.1X User, click **Security > 802.1X > 802.1X User**:

Figure 5 - 20. 802.1X User window

Authentication RADIUS Server

The RADIUS feature of the Switch allows you to facilitate centralized user administration as well as providing protection against a sniffing, active hacker.

To configure the 802.1X User, click **Security > 802.1X > Authentication RADIUS Server**:

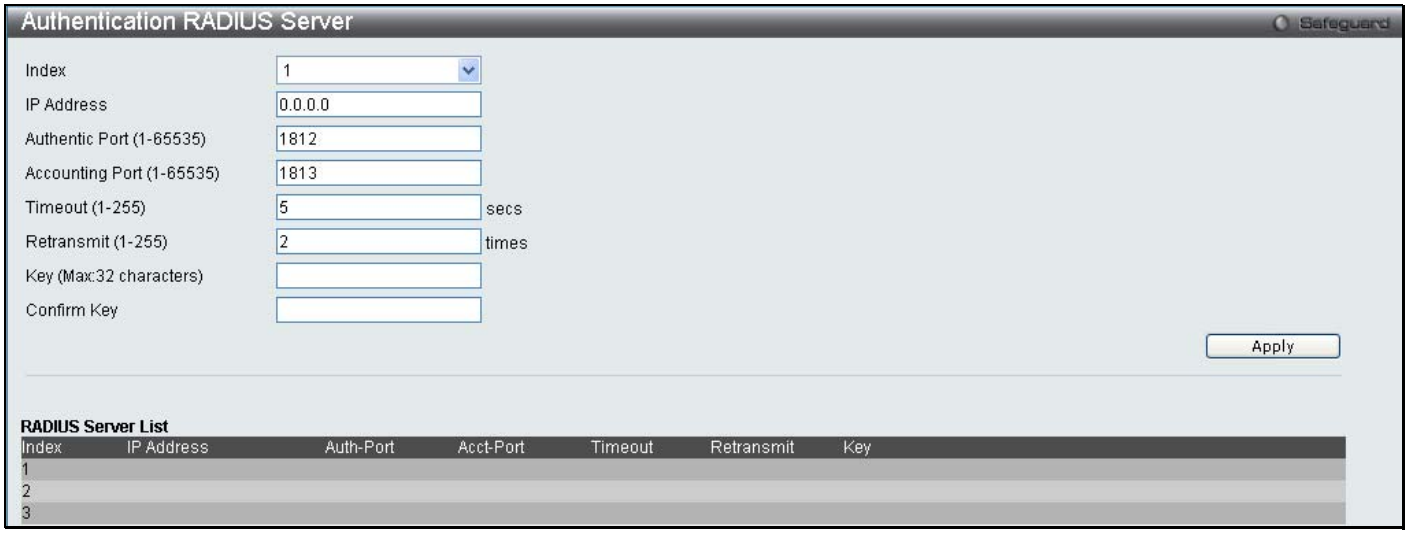


Figure 5 - 21. Authentication RADIUS Server window

This window displays the following information:

Parameter	Description
Index	Choose the desired RADIUS server to configure: *1, 2* or *3*.
IP Address	Set the RADIUS Server IP.
Authentic Port (1-65535)	Set the RADIUS authentic server(s) UDP port. The default port is *1812*.
Accounting Port (1-65535)	Set the RADIUS account server(s) UDP port. The default port is *1813*.
Timeout (1-255)	Enter the timeout value in seconds (*1* to *255*) the default value is *5*.
Retransmit (1-255)	Set the retransmit value in seconds (*1* to *255*) the default value is *2*.
Key (Max. length 32 bytes)	Set the key the same as that of the RADIUS server. Maximum length of the entry is 32 bytes.

Guest VLAN Configuration

On 802.1X security enabled networks, there is a need for non 802.1X supported devices to gain limited access to the network, due to lack of the proper 802.1X software or incompatible devices, such as computers running Windows 98 or lower operating systems, or the need for guests to gain access to the network without full authorization. To supplement these circumstances, this switch now implements 802.1X Guest VLANs. These VLANs should have limited access rights and features separate from other VLANs on the network.

To implement 802.1X Guest VLANs, the user must first create a VLAN on the network with limited rights and then enable it as an 802.1X guest VLAN. Then the administrator must configure the guest accounts accessing the Switch to be placed in a Guest VLAN when trying to access the Switch. Upon initial entry to the Switch, the client wishing services on the Switch will need to be authenticated by a remote RADIUS Server or local authentication on the Switch to be placed in a fully operational VLAN. If authenticated and the authenticator posseses the VLAN placement information, that client will be accepted into the fully operational target VLAN and normal switch functions will be open to the client. If the authenticator does not have target VLAN placement information, the client will be returned to its originating VLAN. Yet, if the client is denied authentication by the authenticator, it will be placed in the Guest VLAN where it has limited rights and access. The adjacent figure should give the user a better understanding of the Guest VLAN process.

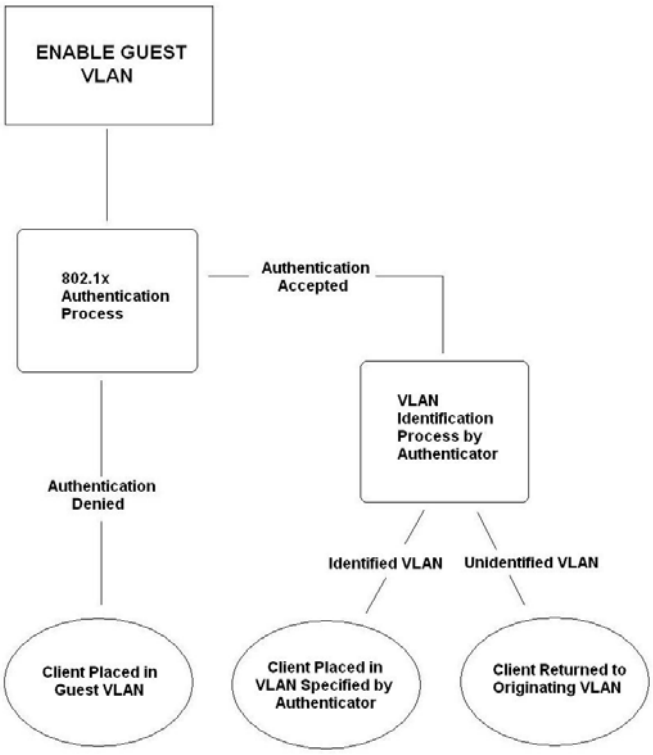


Figure 5 - 22. Guest VLAN Authentication Process

Limitations Using the Guest VLAN

1. Ports supporting Guest VLANs cannot be GVRP enabled and vice versa.
2. A port cannot be a member of a Guest VLAN and a static VLAN simultaneously.
3. Once a client has been accepted into the target VLAN, it can no longer access the Guest VLAN.
4. If a port is a member of multiple VLANs, it cannot become a member of the Guest VLAN.

Guest VLAN

To view the following window, click, **Security > 802.1X > Guest VLAN**:

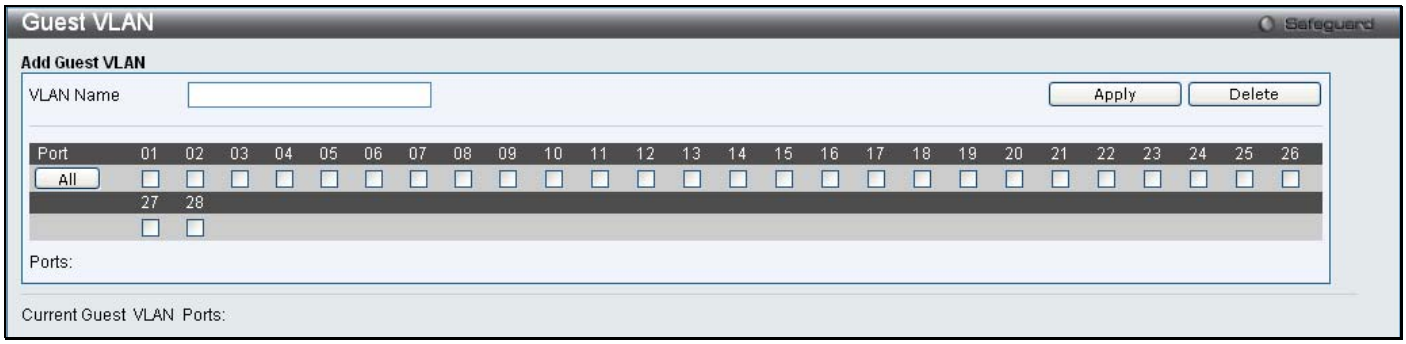

Guest VLAN
Safeguard
Add Guest VLAN
VLAN Name
Apply
Delete
Port 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
All
27 28
Ports:
Current Guest VLAN Ports:

Figure 5 - 23. Guest VLAN window

The following fields may be modified to enable the 802.1X Guest VLAN:

Parameter	Description
VLAN Name	Enter the pre-configured VLAN name to create as an 802.1X Guest VLAN.
Port List	Set the individual port(s) to be enabled for the 802.1X Guest VLAN or click **All**.

Click **Apply** to implement the 802.1X Guest VLAN. Once properly configured, the Guest VLAN Name and associated ports will be listed in the lower part of the window.

NOTE: For more information and configuration examples for the 802.1X Guest VLAN function, please refer to the Guest VLAN Configuration Example located on the D-Link Website.

Initialize Port(s)

Existing 802.1X port and MAC-based settings are displayed and can be configured using the two windows below.

To initialize ports for the port side of 802.1X, the user must first enable 802.1X by port in the **802.1X Settings** window.

To view the following window, click **Security > 802.1X > Initialize Port(s)**:

Figure 5 - 24. Initialize Port(s) window for Port-based 802.1X

This window allows initialization of a port or group of ports. The Initialize Port Table in the bottom half of the window displays the current status of the port(s). To initialize ports, choose the range of ports in the From Port and To Port fields. To begin the initialization, click **Apply**.

To initialize ports for the MAC-based side of 802.1X, the user must first enable 802.1X by MAC address in the **802.1X Settings** window.

To view the following window, click **Security > 802.1X > Initialize Port(s)**:

Figure 5 - 25. Initialize Port(s) window for MAC-based 802.1X

To initialize ports, choose the range of ports in the From Port and To Port fields. Next, the user must specify the MAC address to be initialized by entering it into the MAC Address field and ticking the corresponding check box. To begin the initialization, click **Apply**.

NOTE: The user must first globally enable 802.1X in the **802.1X Settings** window (**Security** > **802.1X** > **802.1X Settings**) before initializing ports. Information in the **Initialize Port(s)** windows cannot be viewed before enabling 802.1X for either Port-based 802.1X or MAC-based 802.1X.

The **Initalize Port(s)** windows display the following information:

Parameter	Description
From Port	The beginning port in a range of ports to be initialized.
To Port	The ending port in a range of ports to be initialized.
Port	A read-only field indicating a port on the Switch.
Auth PAE State	The Authenticator PAE State will display one of the following: *Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth,* and *N/A.*
Backend_State	The Backend Authentication State will display one of the following: *Request, Response, Success, Fail, Timeout, Idle, Initialize,* and *N/A.*
Port Status	The status of the controlled port can be *Authorized, Unauthorized,* or *N/A.*
MAC Address	The authenticated MAC address of the client connected to the corresponding port, if any.

Reauthenticate Port(s)

Users can display and configure reauthenticate ports for 802.1X port and MAC-based using the two windows below.

To reauthenticate ports for the port side of 802.1X, the user must first enable 802.1X by port in the **802.1X Settings** window

To view the following window, click **Security > 802.1X > Reauthenticate Port(s)**:

Figure 5 - 26. Reauthenticate Port(s) window for Port-based 802.1X

This window allows reauthentication of a port or group of ports by using the drop-down menus From Port and To Port and clicking **Apply**. The Reauthenticate Port Table displays the current status of the reauthenticated port(s) once **Apply** has been clicked**.**

NOTE: The user must first globally enable 802.1X in the **802.1X Settings** window (**Security** > **802.1X** > **802.1X Settings**) before reauthenticating ports. Information in the **Reauthenticate Port(s)** window cannot be viewed before enabling 802.1X.

To reauthenticate ports for the MAC-based side of 802.1X, the user must first enable 802.1X by MAC address in the **802.1X Settings** window.

To view the following window, click **Security > 802.1X > Reauthenticate Port(s)**:

Figure 5 - 27. Reauthenticate Port(s) window for MAC-based 802.1X

To reauthenticate ports, first use the From Port and To Port drop-down menus to choose the range of ports. Then the user must specify the MAC address to be reauthenticated by entering it into the MAC Address field and ticking the corresponding check box. To begin the reauthentication, click **Apply**.

This window displays the following information:

Parameter	Description
From Port	The beginning port in a range of ports to be reauthenticated.
To Port	The ending port in a range of ports to be reauthenticated.
MAC Address	Displays the physical address of the Switch where the port resides.
Auth PAE State	The Authenticator State will display one of the following: *Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth,* and *N/A.*
Backend_State	The Backend State will display one of the following: *Request, Response, Success, Fail, Timeout, Idle, Initialize,* and *N/A.*
Port Status	The status of the controlled port can be *Authorized, Unauthorized,* or *N/A*.

SSL Settings

Secure Sockets Layer or SSL is a security feature that will provide a secure communication path between a host and client through the use of authentication, digital signatures and encryption. These security functions are implemented through the use of a *ciphersuite*, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session and consists of three levels:

1. **Key Exchange:** The first part of the cyphersuite string specifies the public key algorithm to be used. This switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the *DHE DSS* Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and host as they "exchange keys" in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.
2. **Encryption:** The second part of the ciphersuite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:
    - Stream Ciphers – There are two types of stream ciphers on the Switch, *RC4 with 40-bit keys* and *RC4 with 128-bit keys*. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.
    - CBC Block Ciphers – CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the *3DES EDE* encryption code defined by the Data Encryption Standard (DES) to create the encrypted text.
3. **Hash Algorithm**: This part of the ciphersuite allows the user to choose a message digest function which will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch supports two hash algorithms, *MD5* (Message Digest 5) and *SHA* (Secure Hash Algorithm).

These three parameters are uniquely assembled in four choices on the Switch to create a three-layered encryption code for secure communication between the server and the host. The user may implement any one or combination of the ciphersuites available, yet different ciphersuites will affect the security level and the performance of the secured connection. The information included in the ciphersuites is not included with the Switch and requires downloading from a third source in a file form called a *certificate*. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server. The Switch

supports SSLv3 and TLSv1. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to host.

Download Certificate

This window is used to download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. The Switch only supports certificate files with .der file extensions. The Switch is shipped with a certificate pre-loaded though the user may need to download more, depending on user circumstances.

Ciphersuite

This window will allow the user to enable SSL on the Switch and implement any one or combination of listed ciphersuites on the Switch. A *ciphersuite* is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The Switch possesses four possible ciphersuites for the SSL function, which are all enabled by default. To utilize a particular ciphersuite, disable the unwanted ciphersuites, leaving the desired one for authentication.

When the SSL function has been enabled, the web will become disabled. To manage the Switch through the web based management while utilizing the SSL function, the web browser must support SSL encryption and the header of the URL must begin with https://. (Ex. https://10.90.90.90) Any other method will result in an error and no access can be authorized for the web-based management.

To view this window, click **Security > SSL Settings**:

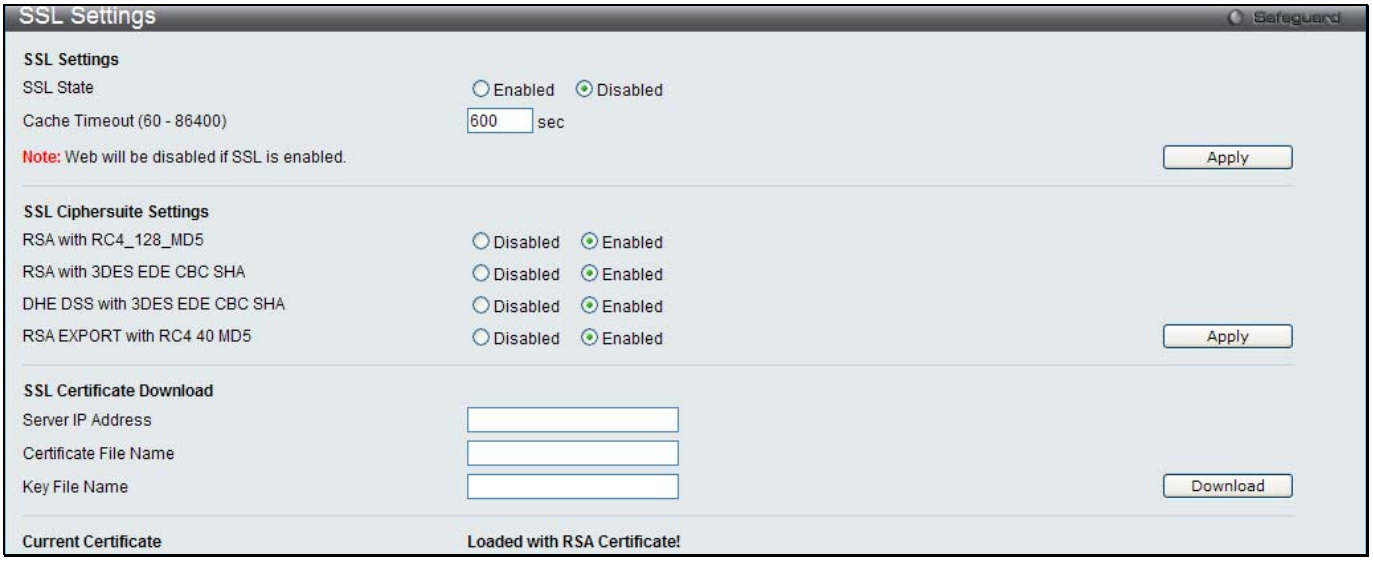


Figure 5 - 28. SSL Settings window

To set up the SSL function on the Switch, configure the following parameters and click **Apply**.

Parameter	Description
SSL Settings	
SSL Status	*Enable* or *Disable* the SSL status on the switch. The default is disabled.
Cache Timeout (60-86400)	This field will set the time between a new key exchange between a client and a host using the SSL function. A new SSL session is established every time the client and host go through a key exchange. Specifying a longer timeout will allow the SSL session to reuse the master key on future connections with that particular host, therefore speeding up the negotiation process. The default setting is *600* seconds.
SSL Ciphersuite Settings	

RSA with RC4_128_MD5	This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is enabled by default.
RSA with 3DES EDE CBC SHA	This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is enabled by default.
DHE DSS with 3DES EDE CBC SHA	This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is enabled by default.
RSA EXPORT with RC4 40 MD5	This ciphersuite combines the RSA Export key exchange and stream cipher RC4 encryption with 40-bit keys. Use the pull-down menu to enable or disable this ciphersuite. This field is enabled by default.
SSL Certificate Download	
Server IP Address	Enter the IP address of the TFTP server where the certificate files are located.
Certificate File Name	Enter the path and the filename of the certificate file to download. This file must have a .der extension. (Ex. c:/cert.der)
Key File Name	Enter the path and the filename of the key file to download. This file must have a .der extension (Ex. c:/pkey.der)

NOTE: Enabling the SSL command will disable the web-based switch management. To log on to the Switch again, the header of the URL must begin with https://. Entering anything else into the address field of the web browser will result in an error and no authentication will be granted.

SSH

SSH is an abbreviation of Secure Shell, which is a program allowing secure remote login and secure network services over an insecure network. It allows a secure login to remote host computers, a safe method of executing commands on a remote end node, and will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now threaten network communications.

The steps required to use the SSH protocol for secure communication between a remote PC (the SSH client) and the Switch (the SSH server) are as follows:

1. Create a user account with admin-level access using the User Accounts window in the **Configuration** folder. This is identical to creating any other admin-level User Account on the Switch, including specifying a password. This password is used to logon to the Switch, once a secure communication path has been established using the SSH protocol.
2. Configure the User Account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the **SSH User Authentication** window. There are three choices as to the method SSH will use to authorize the user, which are *Host Based*, *Password* and *Public Key*.
3. Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH client and the SSH server, using the **SSH Authmode and Algorithm Settings** window.
4. Finally, enable SSH on the Switch using the **SSH Settings** window.

After completing the preceding steps, a SSH Client on a remote PC can be configured to manage the Switch using a secure, in band connection.

SSH Settings

The following window is used to configure and view settings for the SSH server.

To view this window, click **Security > SSH > SSH Settings**:

Figure 5 - 29. SSH Settings window

To configure the SSH server on the Switch, modify the following parameters and click **Apply**:

Parameter	Description
SSH Server State	Enable or disable SSH on the Switch. The default is *Disabled*.
Max Session (1-8)	Enter a value between *1* and *8* to set the number of users that may simultaneously access the Switch. The default setting is *8*.
Connection Timeout (120-600)	Allows the user to set the connection timeout. The use may set a time between *120* and *600* seconds. The default setting is *120* seconds.
Authfail Attempts (2-20)	Allows the Administrator to set the maximum number of attempts that a user may try to log on to the SSH Server utilizing the SSH authentication. After the maximum number of attempts has been exceeded, the Switch will be disconnected and the user must reconnect to the Switch to attempt another login. The number of maximum attempts may be set between *2* and *20*. The default setting is *2*.
Rekey Timeout	Using the pull-down menu uses this field to set the time period that the Switch will change the security shell encryptions. The available options are *Never*, *10 min*, *30 min*, and *60 min*. The default setting is *Never*.

Click **Apply** to implement changes made.

SSH Authmode and Algorithm Settings

The SSH Algorithm window allows the configuration of the desired types of SSH algorithms used for authentication encryption. There are four categories of algorithms listed and specific algorithms of each may be enabled or disabled by checking the boxes. All algorithms are enabled by default.

To view this window, click **Security > SSH > SSH Authmode and Algorithm Settings**:

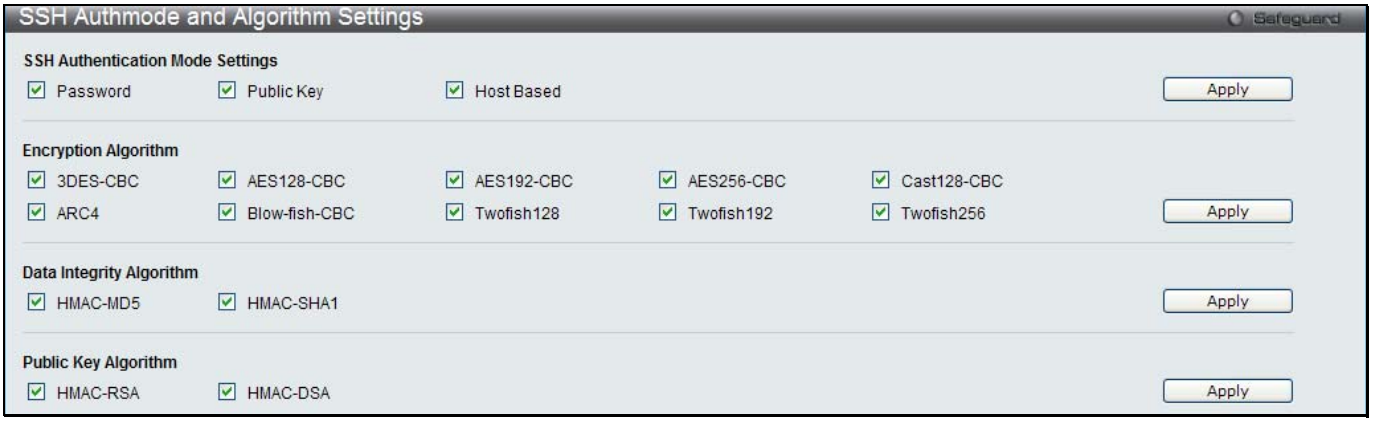


Figure 5 - 30. SSH Authmode and Algorithm Settings window

The following algorithms may be set:

Parameter	Description
SSH Authentication Mode Settings	
Password	This parameter may be enabled if the administrator wishes to use a locally configured password for authentication on the Switch. The default is enabled.
Public Key	This parameter may be enabled if the administrator wishes to use a public key configuration set on a SSH server, for authentication on the Switch. The default is enabled.
Host-based	This parameter may be enabled if the administrator wishes to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed. The default is enabled.
Encryption Algorithm	
3DES-CBC	Tick the check box to enable the Triple Data Encryption Standard encryption algorithm with Cipher Block Chaining. The default is enabled.
Blow-fish CBC	Tick the check box to enable the Blowfish encryption algorithm with Cipher Block Chaining. The default is enabled.
AES128-CBC	Tick the check box to enable the Advanced Encryption Standard AES128 encryption algorithm with Cipher Block Chaining. The default is enabled.
AES192-CBC	Tick the check box to enable the Advanced Encryption Standard AES192 encryption algorithm with Cipher Block Chaining. The default is enabled.
AES256-CBC	Tick the check box to enable the Advanced Encryption Standard AES-256 encryption algorithm with Cipher Block Chaining. The default is enabled.
ARC4	Tick the check box to enable the Arcfour encryption algorithm with Cipher Block Chaining. The default is enabled.
Cast128-CBC	Tick the check box to enable the Cast128 encryption algorithm with Cipher Block Chaining. The default is enabled.
Twofish128	Tick the check box to enable the twofish128 encryption algorithm. The default is enabled.
Twofish192	Tick the check box to enable the twofish192 encryption algorithm. The default is enabled.
Twofish256	Tick the check box to enable the twofish256 encryption algorithm. The default is enabled.
Data Integrity Algorithm	
HMAC-SHA1	Tick the check box to enable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Secure Hash algorithm. The default is enabled.
HMAC-MD5	Tick the check box to enable the HMAC (Hash for Message Authentication Code) mechanism utilizing the MD5 Message Digest encryption algorithm. The default is enabled.

Public Key Algorithm	
HMAC-RSA	Tick the check box to enable the HMAC (Hash for Message Authentication Code) mechanism utilizing the RSA encryption algorithm. The default is enabled.
HMAC-DSA	Tick the check box to enable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Digital Signature Algorithm encryption. The default is enabled.

Click **Apply** to implement changes made.

SSH User Authentication Lists

The following windows are used to configure parameters for users attempting to access the Switch through SSH.

To access the following window, click **Security > SSH > SSH User Authentication Lists**:

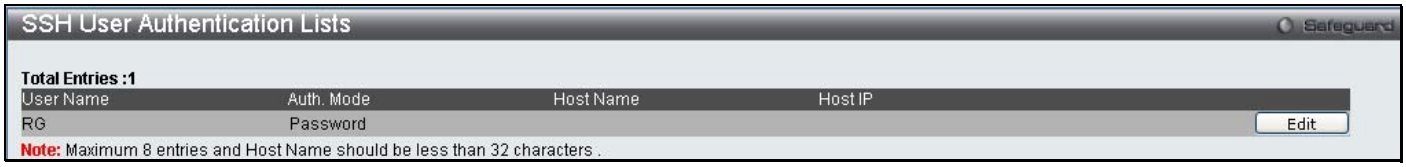


Figure 5 - 31. SSH User Authentication Lists window

In the example above, the User Account “RG” has been previously set using the **User Accounts** window in the **Configuration** folder. A User Account MUST be set in order to set the parameters for the SSH user. To edit the parameters for a SSH user, click on the corresponding **Edit** button, which will reveal the following window to configure:

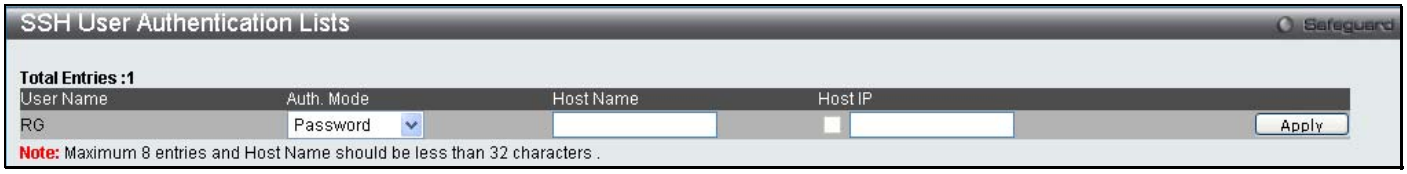


Figure 5 - 32. SSH User Authentication Lists (Edit) window

The user may set the following parameters:

Parameter	Description
User Name	Enter a User Name of no more than 15 characters to identify the SSH user. This User Name must be a previously configured user account on the Switch.
Auth. Mode	The administrator may choose one of the following to set the authorization for users attempting to access the Switch. *Host Based* – This parameter should be chosen if the administrator wishes to use a remote SSH server for authentication purposes. Choosing this parameter requires the user to input the following information to identify the SSH user. *Host Name* – Enter an alphanumeric string of no more than 32 characters to identify the remote SSH user. *Host IP* – Enter the corresponding IP address of the SSH user. *Password* – This parameter should be chosen if the administrator wishes to use an administrator-defined password for authentication. Upon entry of this parameter, the Switch will prompt the administrator for a password, and then to re-type the password for confirmation. *Public Key* – This parameter should be chosen if the administrator wishes to use the publickey on a SSH server for authentication.
Host Name	Enter an alphanumeric string of no more than 32 characters to identify the remote SSH user. This parameter is only used in conjunction with the Host Based choice in the Auth. Mode field.
Host IP	Enter the corresponding IP address of the SSH user. This parameter is only used in

	conjunction with the Host Based choice in the Auth. Mode field.

Click **Apply** to implement changes made.

NOTE: To set the SSH User Authentication parameters on the Switch, a User Account must be previously configured. For more information on configuring local User Accounts on the Switch, see the User Accounts section of this manual located in the Configuration section.

Access Authentication Control

The TACACS/XTACACS/TACACS+/RADIUS commands allow users to secure access to the Switch using the TACACS/XTACACS/TACACS+/RADIUS protocols. When a user logs in to the Switch or tries to access the administrator level privilege, he or she is prompted for a password. If TACACS/XTACACS/TACACS+/RADIUS authentication is enabled on the Switch, it will contact a TACACS/XTACACS/TACACS+/RADIUS server to verify the user. If the user is verified, he or she is granted access to the Switch.

There are currently three versions of the TACACS security protocol, each a separate entity. The Switch's software supports the following versions of TACACS:

TACACS (Terminal Access Controller Access Control System) - Provides password checking and authentication, and notification of user actions for security purposes utilizing via one or more centralized TACACS servers, utilizing the UDP protocol for packet transmission.

Extended TACACS (XTACACS) - An extension of the TACACS protocol with the ability to provide more types of authentication requests and more types of response codes than TACACS. This protocol also uses UDP to transmit packets.

TACACS+ (Terminal Access Controller Access Control System plus) - Provides detailed access control for authentication for network devices. TACACS+ is facilitated through Authentication commands via one or more centralized servers. The TACACS+ protocol encrypts all traffic between the Switch and the TACACS+ daemon, using the TCP protocol to ensure reliable delivery

In order for the TACACS/XTACACS/TACACS+/RADIUS security function to work properly, a TACACS/XTACACS/TACACS+/RADIUS server must be configured on a device other than the Switch, called an Authentication Server Host and it must include usernames and passwords for authentication. When the user is prompted by the Switch to enter usernames and passwords for authentication, the Switch contacts the TACACS/XTACACS/TACACS+/RADIUS server to verify, and the server will respond with one of three messages:

The server verifies the username and password, and the user is granted normal user privileges on the Switch.

The server will not accept the username and password and the user is denied access to the Switch.

The server doesn't respond to the verification query. At this point, the Switch receives the timeout from the server and then moves to the next method of verification configured in the method list.

The Switch has four built-in Authentication Server Groups, one for each of the TACACS, XTACACS, TACACS+ and RADIUS protocols. These built-in Authentication Server Groups are used to authenticate users trying to access the Switch. The users will set Authentication Server Hosts in a preferable order in the built-in Authentication Server Groups and when a user tries to gain access to the Switch, the Switch will ask the first Authentication Server Hosts for authentication. If no authentication is made, the second server host in the list will be queried, and so on. The built-in Authentication Server Groups can only have hosts that are running the specified protocol. For example, the TACACS Authentication Server Groups can only have TACACS Authentication Server Hosts.

The administrator for the Switch may set up six different authentication techniques per user-defined method list (TACACS/XTACACS/TACACS+/RADIUS/local/none) for authentication. These techniques will be listed in an order preferable, and defined by the user for normal user authentication on the Switch, and may contain up to eight authentication techniques. When a user attempts to access the Switch, the Switch will select the first technique listed for authentication. If the first technique goes through its Authentication Server Hosts and no authentication is returned, the Switch will then go to the next technique listed in the server group for authentication, until the authentication has been verified or denied, or the list is exhausted.

Please note that when the user logins to the device successfully through TACACS/XTACACS/TACACS+server or none method, the “user” priviledge level is the only level assigned. If the user wants to get the administration privilege level, the user must use the “enable admin” command to promote his privilege level. However when the user logins to

the device successfully through the RADIUS server or through the local method, 3 kinds of privilege levels can be assigned to the user and the user can not use the “enable admin” command to promote to the admin privilege level.

NOTE: TACACS, XTACACS and TACACS+ are separate entities and are not compatible. The Switch and the server must be configured exactly the same, using the same protocol. (For example, if the Switch is set up for TACACS authentication, so must be the host server.)

Authentication Policy Settings

This window offers an administrator-defined authentication policy for users trying to access the Switch. When *Enabled*, the device will check the Login Method List and choose a technique for user authentication upon login.

To access the following window, click **Security > Access Authentication Control > Authentication Policy Settings**:

Figure 5 - 33. Authentication Policy Settings window

The following parameters can be set:

Parameters	Description
Authentication Policy	Use the pull-down menu to enable or disable the Authentication Policy on the Switch.
Response Timeout (0-255)	This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between *0* and *255* seconds. The default setting is *30* seconds.
User Attempts (1-255)	This command will configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet and web users will be disconnected from the Switch. The user may set the number of attempts from *1* to *255*. The default setting is *3*.

Click **Apply** to implement changes made.

Application Authentication Settings

This window is used to configure switch configuration applications (console, Telnet, SSH, web) for login at the user level and at the administration level (Enable Admin**)** utilizing a previously configured method list.

To view the following window, click **Security > Access Authentication Control > Application Authentication Settings**:

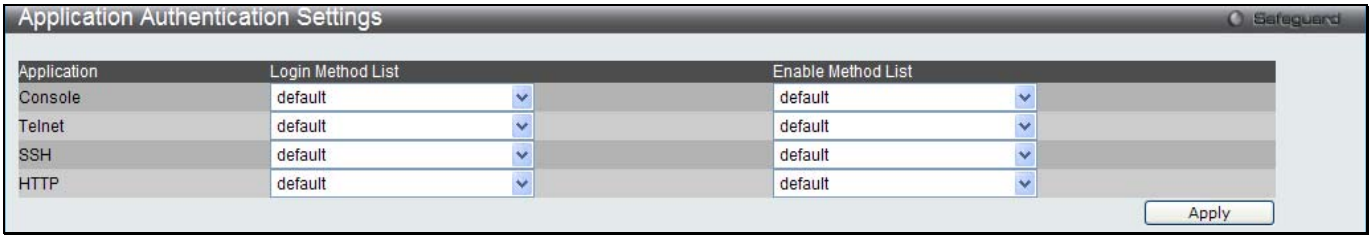


Figure 5 - 34. Application's Authentication Settings window

The following parameters can be set:

Parameter	Description
Application	Lists the configuration applications on the Switch. The user may configure the Login Method List and Enable Method List for authentication for users utilizing the Console (Command Line Interface) application, the Telnet application, SSH, and the WEB (HTTP) application.
Login Method List	Using the pull-down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the **Login Method Lists** window, in this section, for more information.
Enable Method List	Using the pull-down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the **Enable Method Lists** window, in this section, for more information

Click **Apply** to implement changes made.

Authentication Server Group

This window will allow users to set up Authentication Server Groups on the Switch. A server group is a technique used to group TACACS/XTACACS/TACACS+/RADIUS server hosts into user-defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. The Switch has three built-in Authentication Server Groups that cannot be removed but can be modified. Up to eight authentications server hosts may be added to any particular group.

To view the following window, click **Security > Access Authentication Control > Authentication Server Group**:

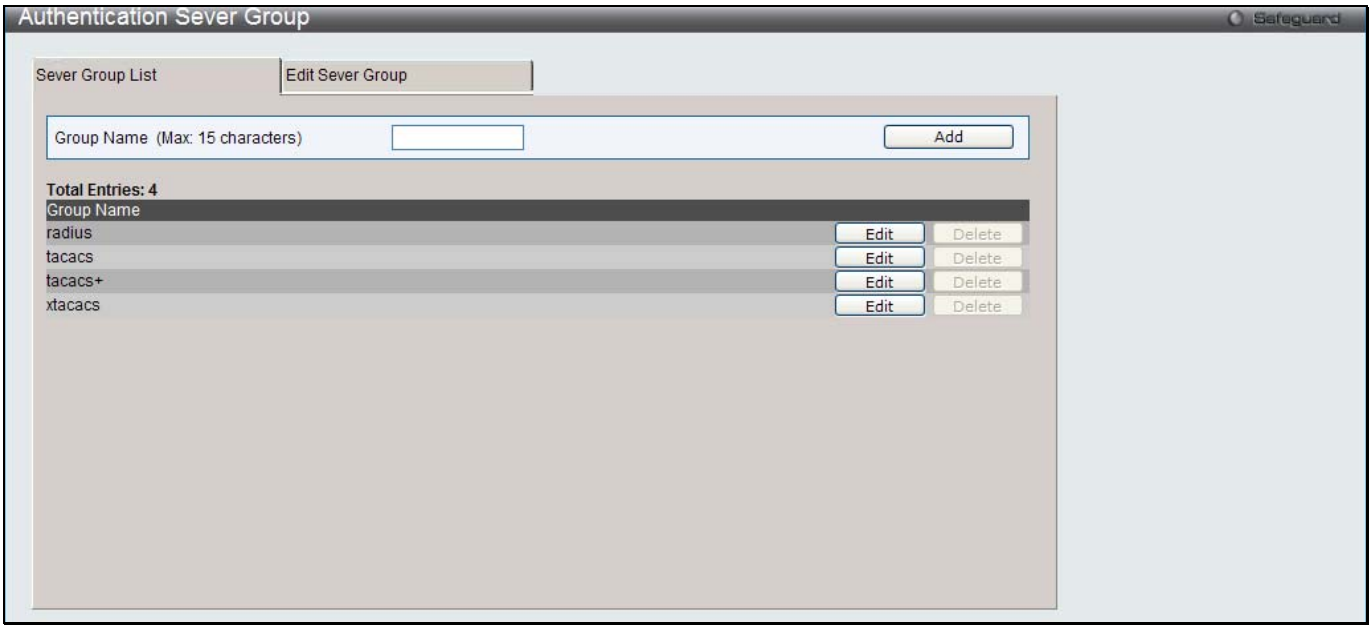


Figure 5 - 35. Authentication Server Group Settings window – Server Group List tab

The Switch has four built-in Authentication Server Groups that cannot be removed but can be modified.

To modify a particular group, click on its corresponding **Edit** button or click the **Edit Server Group** tab at the top of this window, the following tab will be displayed:

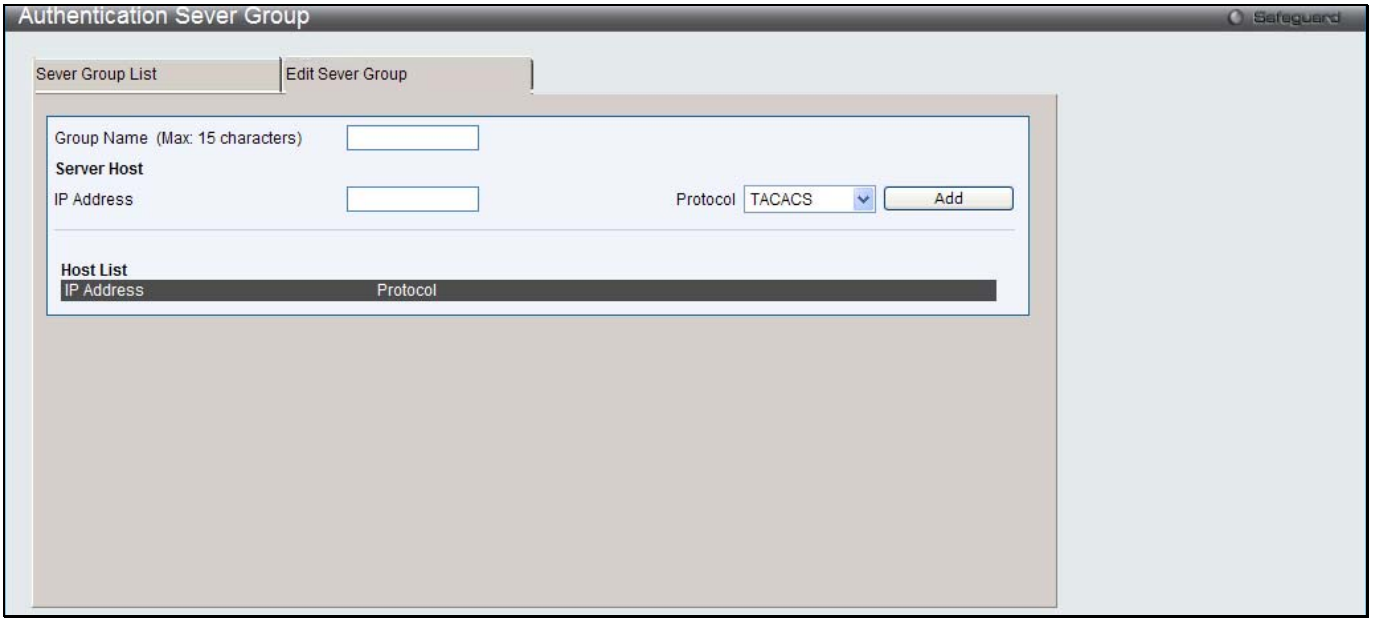


Figure 5 - 36. Authentication Server Group window – Edit Server Group tab

To add an Authentication Server Host to the list, enter its IP address in the IP Address field, choose the protocol associated with the IP address of the Authentication Server Host and click **Add** to add this Authentication Server Host to the group.

NOTE: The user must configure Authentication Server Hosts using the Authentication Server Hosts window before adding hosts to the list. Authentication Server Hosts must be configured for their specific protocol on a remote centralized server before this function can work properly.

NOTE: The four built in server groups can only have server hosts running the same TACACS daemon. TACACS/XTACACS/TACACS+ protocols are separate entities and are not compatible with each other.

Authentication Server

This window will set user-defined Authentication Server Hosts for the TACACS/XTACACS/TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with Authentication Policy enabled, the Switch will send authentication packets to a remote TACACS/XTACACS/TACACS+/RADIUS server host on a remote host. The TACACS/XTACACS/TACACS+/RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.

To view the following window, click **Security > Access Authentication Control > Authentication Server**:

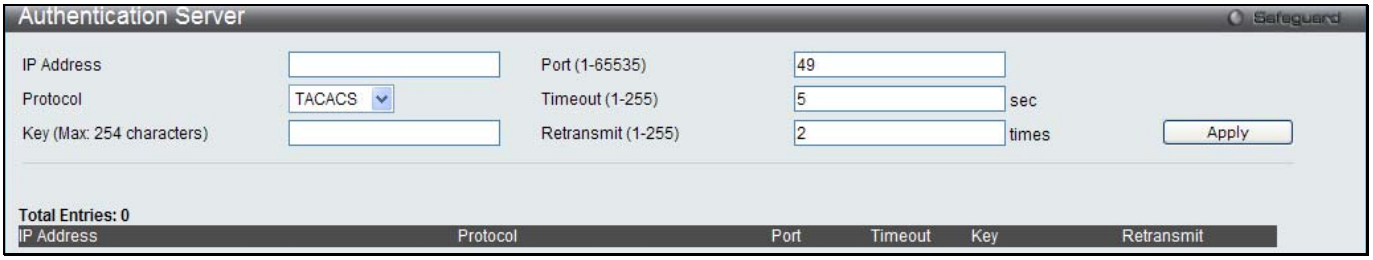


Figure 5 - 37. Authentication Server Settings window

Configure the following parameters to add an Authentication Server Host:

Parameter	Description
IP Address	The IP address of the remote server host the user wishes to add.
Port (1-65535)	Enter a number between *1* and *65535* to define the virtual port number of the authentication protocol on a server host. The default port number is *49* for TACACS/XTACACS/TACACS+ servers and *1813* for RADIUS servers but the user may set a unique port number for higher security.
Protocol	The protocol used by the server host. The user may choose one of the following: *TACACS* - Enter this parameter if the server host utilizes the TACACS protocol. *XTACACS* - Enter this parameter if the server host utilizes the XTACACS protocol. *TACACS+* - Enter this parameter if the server host utilizes the TACACS+ protocol. *RADIUS* - Enter this parameter if the server host utilizes the RADIUS protocol.
Timeout (1-255)	Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is *5* seconds.
Key	Authentication key to be shared with a configured TACACS+ or RADIUS servers only. Specify an alphanumeric string up to 254 characters.
Retransmit (1-255)	Enter the value in the retransmit field to change how many times the device will resend an authentication request when the server does not respond.

Click **Apply** to add the server host. Entries will be displayed in the table on the lower half of this window.

NOTE: More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+ are separate entities and are not compatible with each other

Login Method Lists

This window is used to configure a user-defined or default Login Method List of authentication techniques for users logging on to the Switch. The sequence of techniques implemented in this command will affect the authentication result. For example, if a user enters a sequence of techniques, for example TACACS – XTACACS - local, the Switch will send an authentication request to the first TACACS host in the server group. If no response comes from the server host, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, XTACACS. If no authentication takes place using the XTACACS list, the local account database set in the Switch is used to authenticate the user. When the local method is used, the privilege level will be dependant on the local account privilege configured on the Switch.

When the user logins to the device successfully through TACACS/XTACACS/TACACS+server or none method, the “user” privilege level is assigned only. If the user wants to get admin privilege level, the user must use the **Enable Admin** window to promote his privilege level. (See the Enable Admin part of this section for more detailed information.) But when the user logins to the device successfully through RADIUS server or local method, three kinds of privilege levels can be assigned to the user and the user can not use the **Enable Admin** window to promote to admin privilege level.

To view the following window, click **Security > Access Authentication Control > Login Method Lists**:

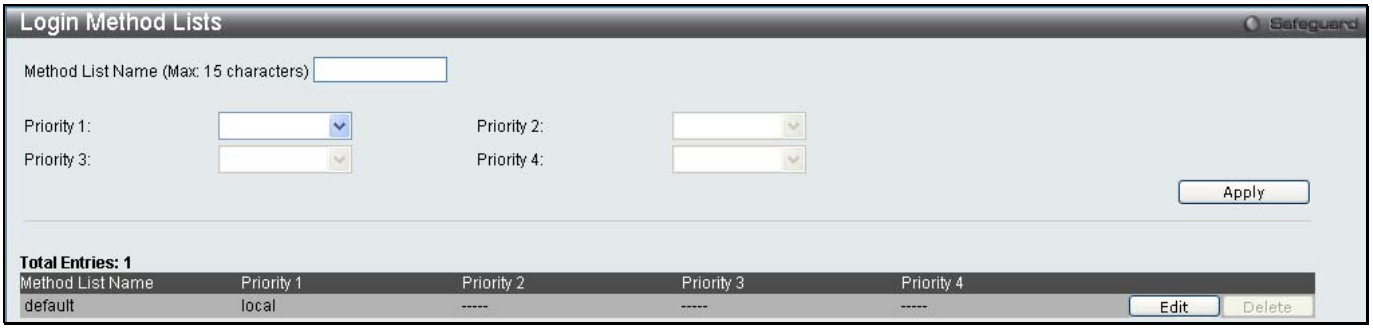


Figure 5 - 38. Login Method Lists window

The Switch contains one Method List that is set and cannot be removed, yet can be modified. To delete a Login Method List defined by the user, click the corressponding **Delete** button. To modify a Login Method List, click on its corresponding **Edit** button.

To define a Login Method List, set the following parameters and click **Apply**:

Parameter	Description
Method List Name	Enter a method list name defined by the user of up to 15 characters.
Priority 1, 2, 3, 4	The user may add one, or a combination of up to four of the following authentication methods to this method list: *tacacs* - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. *xtacacs* - Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server. *tacacs+* - Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server. *radius* - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server. *server_group* - Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch. *local* - Adding this parameter will require the user to be authenticated using the local user account database on the Switch. *none* - Adding this parameter will require no authentication to access the Switch.

Enable Method Lists

This window is used to set up Method Lists to promote users with user level privileges to Administrator (Admin) level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight Enable Method Lists can be implemented on the Switch, one of which is a default Enable Method List. This default Enable Method List cannot be deleted but can be configured.

The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like TACACS - XTACACS - Local Enable, the Switch will send an authentication request to the first TACACS host in the server group. If no verification is found, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, XTACACS. If no authentication takes place using the XTACACS list, the Local Enable password set in the Switch is used to authenticate the user.

Successful authentication using any of these methods will give the user an "Admin" privilege.

NOTE: To set the Local Enable Password, see the next section, entitled Local Enable Password.

To view the following table, click **Security > Access Authentication Control > Enable Method Lists**:

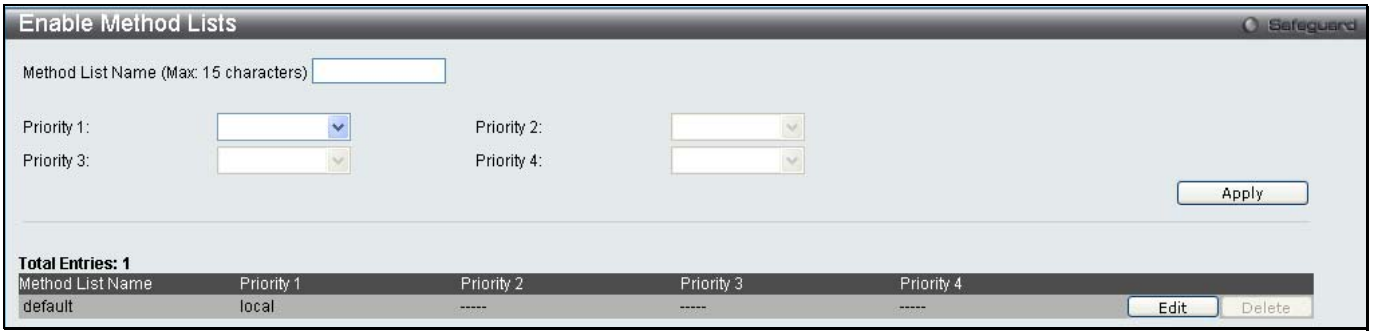


Figure 5 - 39. Enable Method Lists window

To delete an Enable Method List defined by the user, click the the **Delete** button. To modify an Enable Method List, click on its corresponding **Edit** button.

To define an Enable Login Method List, set the following parameters and click **Apply**:

Parameter	Description
Method List Name	Enter a method list name defined by the user of up to 15 characters.
Priority 1, 2, 3, 4	The user may add one, or a combination of up to four of the following authentication methods to this method list: *local_enable* - Adding this parameter will require the user to be authenticated using the local enable password database on the Switch. The user in the next section entitled Local Enable Password must set the local enable password. *none* - Adding this parameter will require no authentication to access the Switch. *radius* - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server. *tacacs* - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. *xtacacs* - Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server. *tacacs+* - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. server_group - Adding a previously configured server group will require the user to be authenticated using a user-defined server group previously configured on the Switch.

Local Enable Password Settings

This window will configure the locally enabled password for the **enable admin** command. When a user chooses the "local_enable" method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here that is locally set on the Switch.

To view the following window, click **Security > Access Authentication Control > Local Enable Password Settings**:

Figure 5 - 40. Local Enable Password Settings window

To set the Local Enable Password, configure the following parameters and click **Apply**:

Parameter	Description
Old Local Enable Password (Max: 15 characters)	If a password was previously configured for this entry, enter it here in order to change it to a new password
New Local Enable Password	Enter the new password that you wish to set on the Switch to authenticate users attempting to access Administrator Level privileges on the Switch. The user may set a password of up to 15 characters.
Confirm Local Enable Password	Confirm the new password entered above. Entering a different password here from the one set in the New Local Enabled field will result in a fail message.

MAC-based Access Control

MAC-based Access Control is a method to authenticate and authorize access using either a port or host. For port-based MAC, the method decides port access rights, while for host-based MAC, the method determines the MAC access rights.

A MAC user must be authenticated before being granted access to a network. Both local authentication and remote RADIUS server authentication methods are supported. In MAC-based Access Control, MAC user information in a local database or a RADIUS server database is searched for authentication. Following the authentication result, users achieve different levels of authorization.

Notes About MAC-based Access Control

There are certain limitations and regulations regarding the MAC-based Access Control:

1. Once this feature is enabled for a port, the Switch will clear the FDB of that port.
2. If a port is granted clearance for a MAC address in a VLAN that is not a Guest VLAN, other MAC addresses on that port must be authenticated for access and otherwise will be blocked by the Switch.
3. Ports that have been enabled for Link Aggregation, Port Security, or GVRP authentication cannot be enabled for MAC-based Authentication.

MAC-based Access Control Settings

The following window is used to set the parameters for the MAC-based Access Control function on the Switch. Here the user can set the running state, method of authentication, RADIUS password, and view the Guest VLAN configuration to be associated with the MAC-based Access Control function of the Switch.

To enable the MAC-based Access Control Global Settings on the Switch, click **Security > MAC-based Access Control > MAC-based Access Control Settings**:

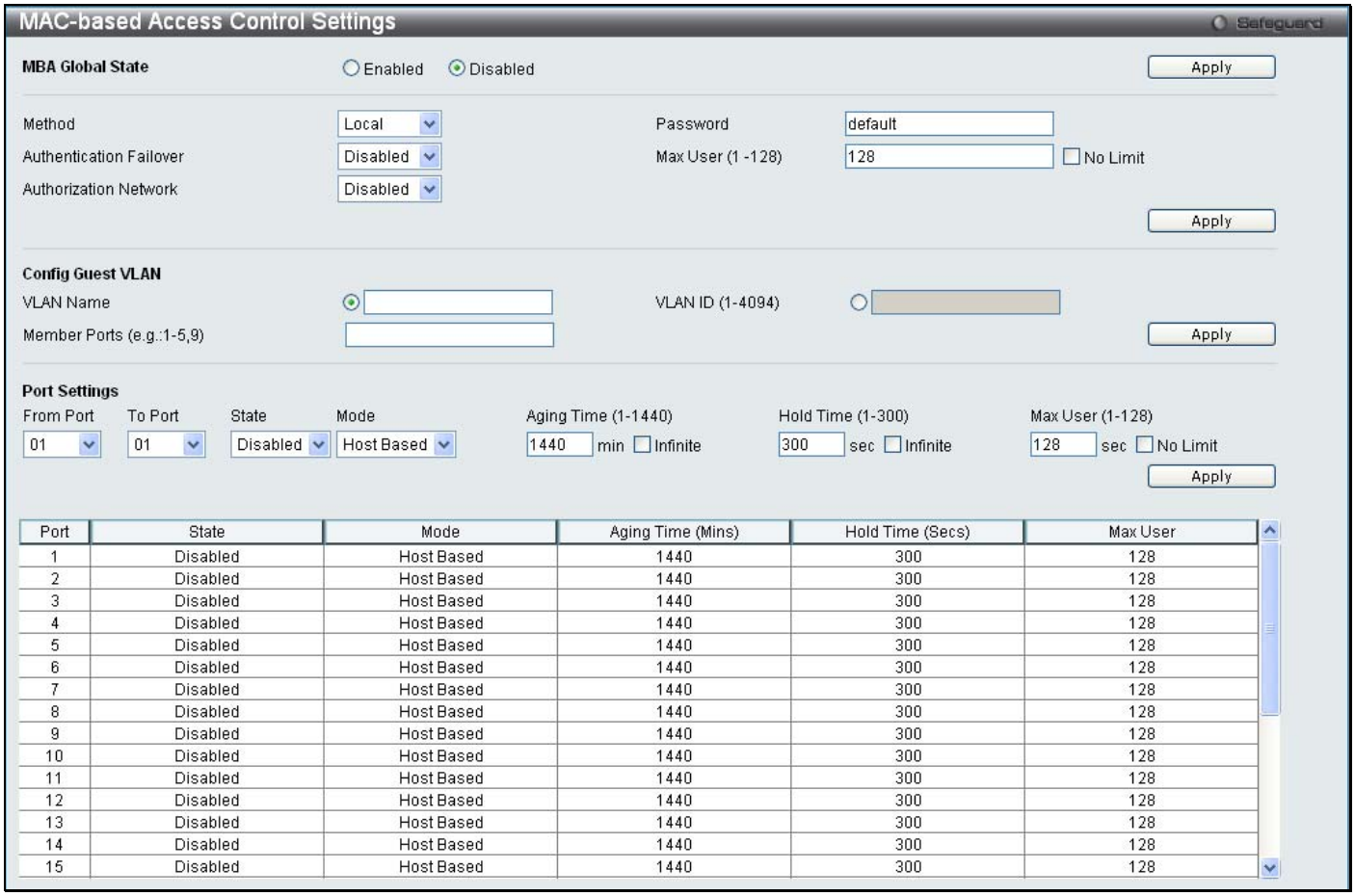


Figure 5 - 41. MAC-based Access Control Settings window

The following parameters may be viewed or set:

Parameter	Description
Settings	
MBA Global State	Use the radio button to globally enable or disable the MAC-based Access Control function on the Switch.
Method	Use the pull-down menu to choose the type of authentication to be used when authentication MAC addresses on a given port. The user may choose between the following methods: *Local* – Use this method to utilize the locally set MAC address database as the authenticator for MAC-based Access Control. This MAC address list can be configured in the MAC-based Access Control Local Database Settings window. *RADIUS* – Use this method to utilize a remote RADIUS server as the authenticator for MAC-based Access Control. Remember, the MAC list must be previously set on the RADIUS server and the settings for the server must be first configured on the Switch.
Password	Enter the password for the RADIUS server, which is to be used for packets being sent requesting authentication. The default password is *default*.
Authentication Failover	By default, authentication failover is *Disabled*. If RADIUS servers are unreachable, authentication will fail. When authentication failover is *Enabled*, if RADIUS server authentication is unreachable, the local database will do the autehtnetication.
Max User (1–128)	Enter a value for the maximum number of users, between *1* and *128*. The default is *128*.
Authorization Network	Enable or disable the Authorization Network.

Config Guest VLAN	
VLAN Name	Enter a Guest VLAN name. Clicking the hyperlinked name will send the Web manager to the Guest VLAN configuration window.
VLAN ID (1-4094)	Enter a VLAN ID number between *1* and *4094*.
Member Ports (e.g.: 1-5, 9)	Displays the list of ports that have been configured for the Guest VLAN.
Port Settings	
From Port/To Port	Enter the Port range.
State	Use the pull-down menu to enable or disable the MAC-based Access Control function on individual ports.
Mode	Toggle between *Port Based* and *Host Based*.
Aging Time (1-1440)	Enter an aging value between *1* and *1440* minutes. The default is *1440.* Tick the Infinite check box for no aging time.
Hold Time (1-300)	Enter a hold value between *1* and *300* seconds. The default is *300*. Tick the Infinite check box for no hold time.
Max User (1-128)	Enter a value for the maximum number of users, between *1* and *128*. The default is *128*. Tick the No Limit check box for no maximum user limit.

MAC-based Access Control Local Settings

The following window is used to set a list of MAC addresses, along with their corresponding target VLAN, which will be authenticated for the Switch. Once a queried MAC address is matched in this table, it will be placed in the VLAN associated with it here. The switch administrator may enter up to 128 MAC addresses to be authenticated using the local method configured here.

To enable the MAC-based Access Control Local MAC Settings on the switch, click **Security > MAC-based Access Control > MAC-based Access Control Local Settings**:

Figure 5 - 42. MAC-based Access Control Local Settings window

To add a MAC address to the local authentication list, enter the MAC address and the target VLAN name into their appropriate fields and click **Add**. To change a MAC address or a VLAN in the list, click the corresponding **Edit By Name** or **Edit By ID** button. To delete a MAC address entry, enter its parameters into the appropriate fields and click **Delete By MAC**, to delete a VLAN, enter its parameters into the appropriate fields and click **Delete By VLAN**. To search for a MAC or a VLAN enter the information in the appropriate fields and click **Find By MAC** or **Find By VLAN**.

DoS Prevention Settings

The Switch supports Denial of Service (DoS) prevention to mitigate DoD attacks from hackers or other malicious sources.

To view this window, click **Security > DoS Prevention Settings**:

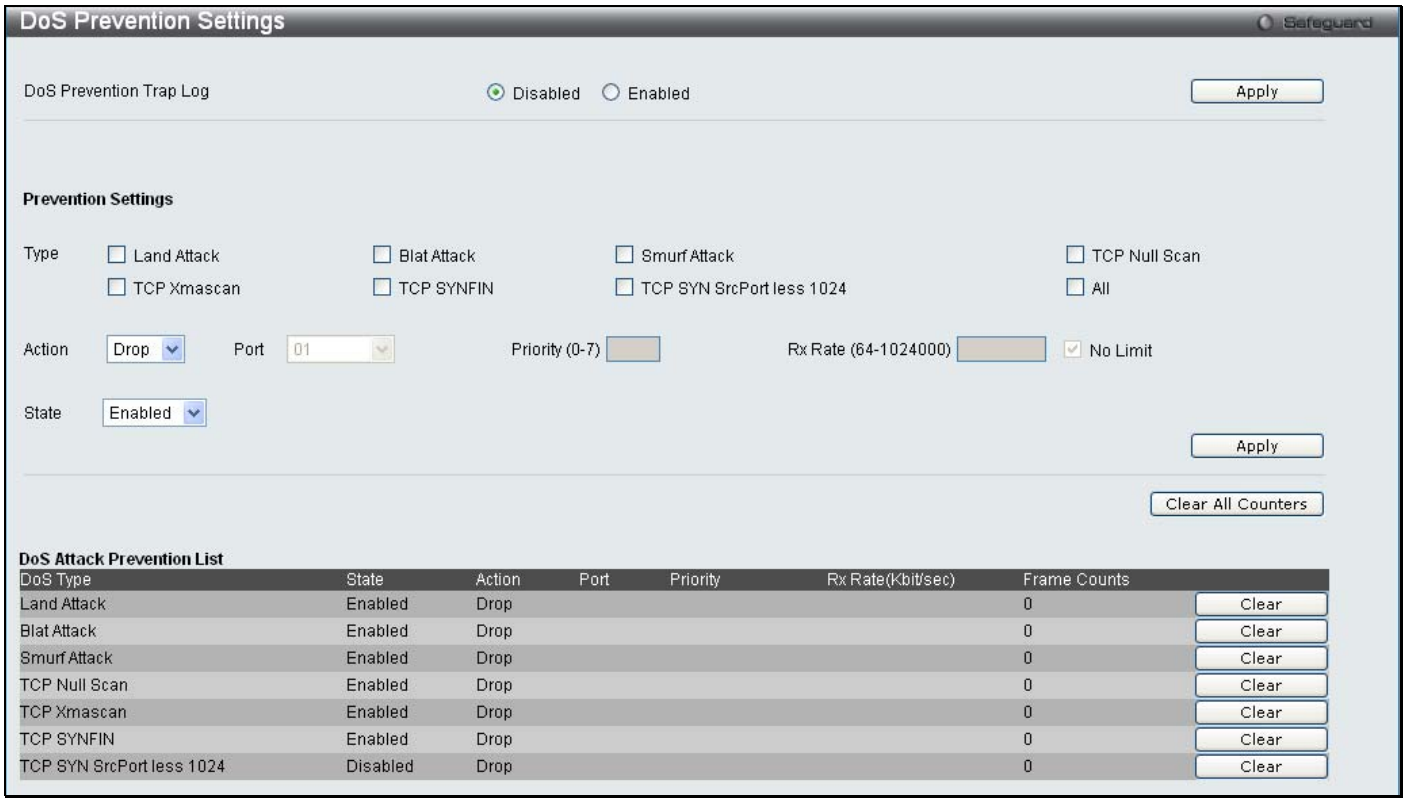


Figure 5 - 43. DoS Prevention Settings window

Set the following parameters and then click **Apply**:

Parameter	Description
DoS Prevention Trap Log	Use the radio button to enable or disable this feature.
Type	Tick the check box for each type of DoS attack: Land Attack, Blat Attack, Smurf Attack, TCP Null Scan, TCP Xmasscan, TCP SYNFIN, TCP SYN SrcPort less 1024, and All.
Action	Toggle between *Drop* and *Mirror*.
Port	Select the Port which the log will be mirrored to.
Priority (0-7)	Select the Priority for the mirror port.
Rx Rate (64-1024000)	Enter a value between *64* and *1024000* or tick the No Limit check box.
State	Toggle to enable or disable DoS Prevention.
Clear	Click to clear the DoS prevention trap logs for the corresponding types of DoS attacks.

Section 6

ACL

ACL Configuration Wizard

Access Profile List

CPU Access Profile List

ACL Finder

ACL Flow Meter

Access profiles allow the user to establish criteria to determine whether or not the Switch will forward packets based on the information contained in each packet's header. These criteria can be specified on a basis of Packet Content, MAC address, or IP address.

ACL Configuration Wizard

This window will aid with the creation of access profiles and ACL Rules. The ACL Wizard will create the access rule and profile automatically.

To view this window click, **ACL > ACL Configuration Wizard**:

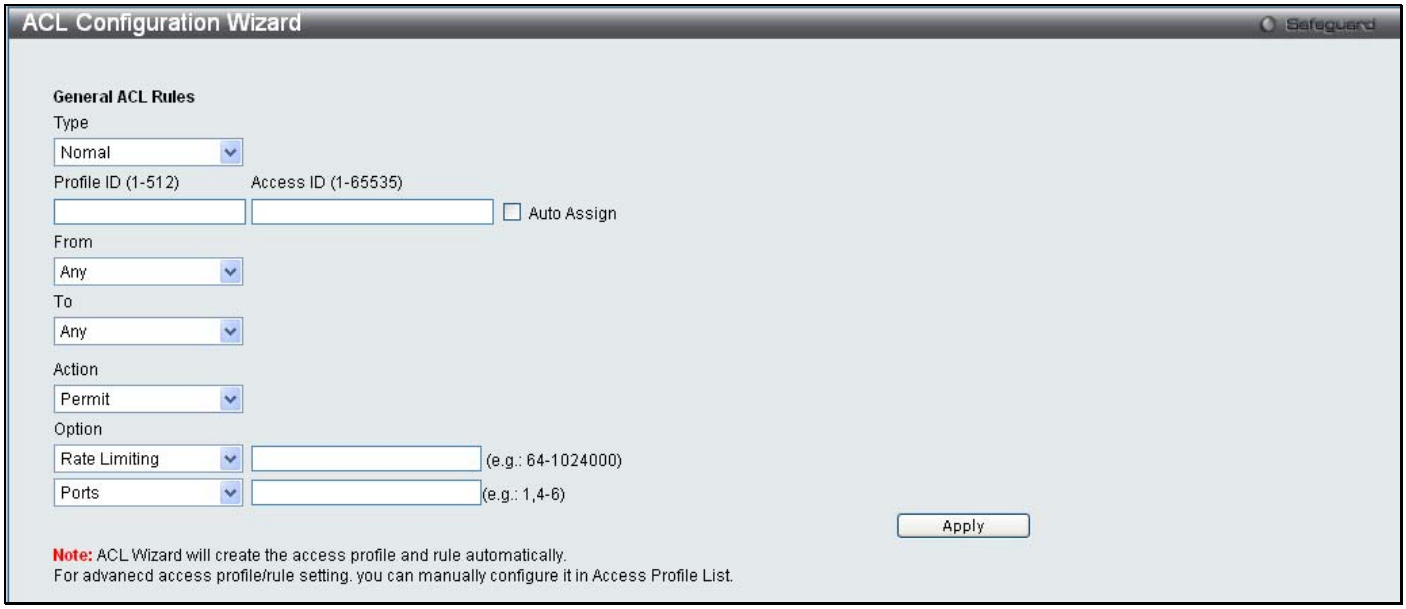


Figure 6 - 1. ACL Configuration Wizard window

The following parameters can be configured:

Parameter	Description
Type	Select the type of ACL you wish to create, either *Normal* or *CPU*.
Profile ID (1-512)	Enter a unique identifier number for this profile set. This value can be set from *1* to *512*.
Access ID (1-65535)	Type in a unique identifier number for this access. This value can be set from *1* to *65535*.
From	Use the drop-down menu to select from *MAC Address*, *IPv4 Address*, *IPv6*, or *Any*.
To	Use the drop-down menu to select from *MAC Address*, *IPv4 Address*, or *Any*. When IPv6 is selected the user can only enter the IPv6 source address or the IPv6 destination address at any one time.

Service Type	Use the drop-down menu to select from *VLAN Name*, *Ethernet Type*, *802.1P*, or *Any*.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify the packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Option	Select between *Rate Limiting*, *Change 1P Priority*, and *Replace DSCP*.
Ports	Enter a range of ports to be configured.

Click **Apply** to implement changes made.

Access Profile List

Creating an access profile is divided into two basic parts. The first is to specify which part or parts of a frame the Switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the Switch will use to determine what to do with the frame. The entire process is described below in two parts.

To display the currently configured Access Profiles on the Switch, click **ACL > Access Profile Lists**:

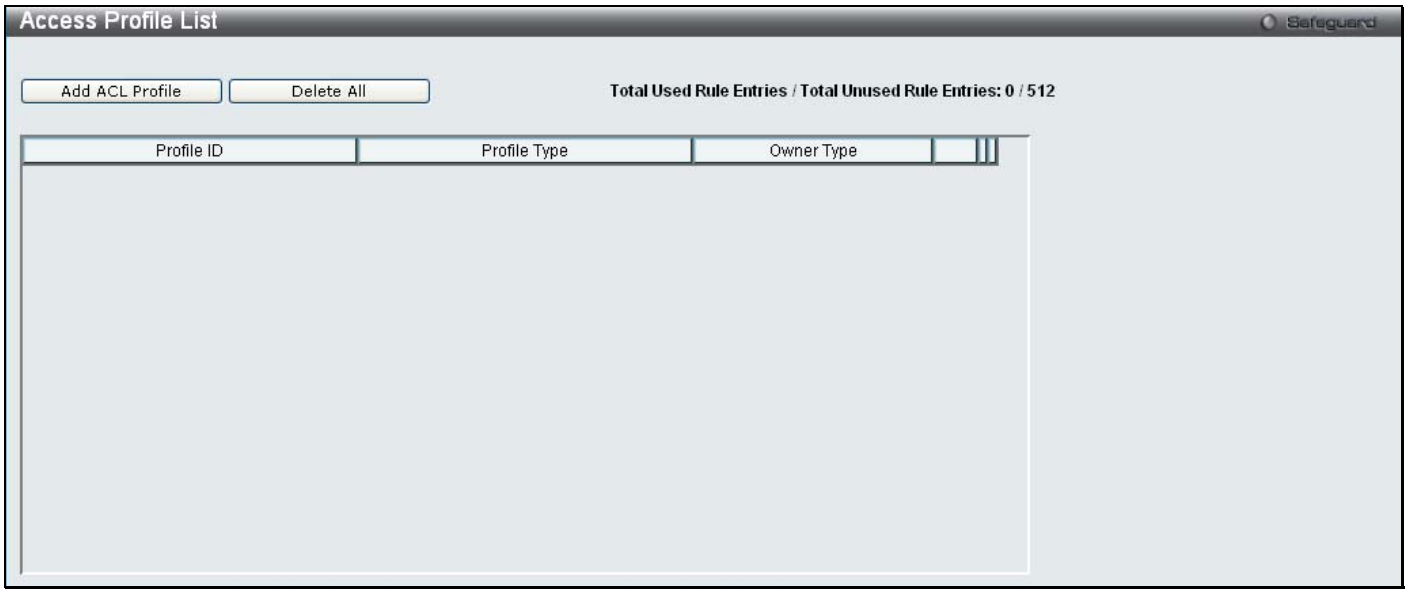


Figure 6 - 2. initial Access Profile List window

To add an ACL Profile, click the **Add ACL Profile** button, which will display the window below:

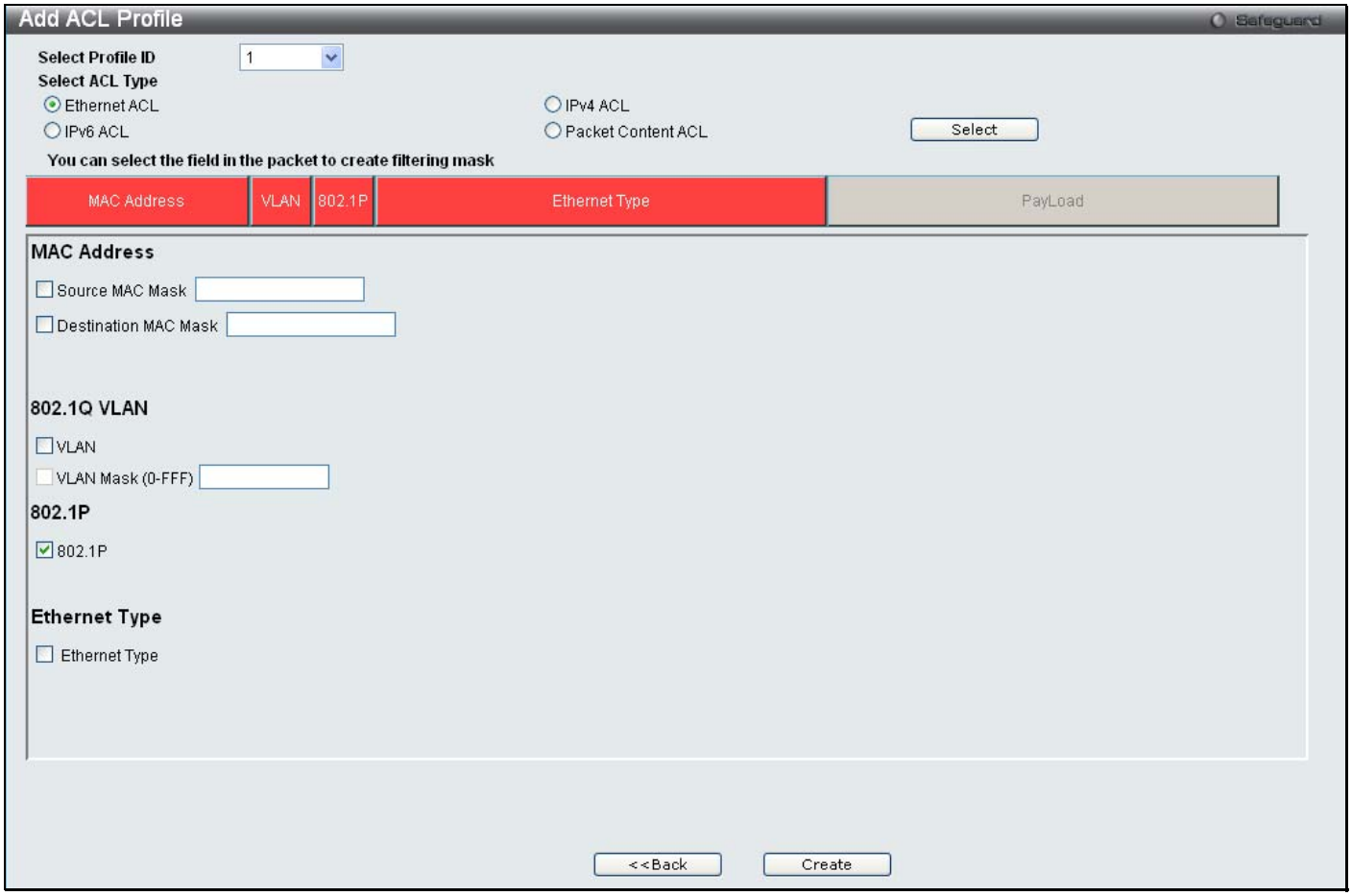


Figure 6 - 3. Add ACL Profile window for Ethernet example

There are four sets of Access Profile configuration windows; one for Ethernet (or MAC address-based) profile configuration, one for IP (IPv4) address-based profile configuration, one for the Packet Content and one for IPv6. Explore the four types of Access Profile configuration options by using the drop-down menu to select a Profile ID between *1* and *512* (*1* has been selected in this example), using the radio button to select an ACL Type (Ethernet ACL has been selected in this example), and then clicking **Select**. Next, click on the boxes near the top of the window, which will then turn red and reveal parameters for configuration (MAC Address, 802.1Q VLAN, 802.1p, and Ethernet Type have been selected in this example). At least one mask must then be selected before clicking the **Create** button (802.1p has been ticked in this example). To return to the Access Profile List window, click **<<Back**.

The following parameters can be configured for Ethernet ACL:

Parameter	Description
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 or packet content mask. This will change the window according to the requirements for the type of profile. Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header. Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header. Select Packet Content ACL to specify a mask to hide the content of the packet header.
MAC Address	Tick either Source MAC Mask and enter the source MAC address mask or Destination MAC Mask and enter the destination MAC address mask.
802.1Q VLAN	VLAN - Specifies a VLAN. VLAN Mask (0-FFF) - Specifies a VLAN mask.

	Selecting this option instructs the Switch to examine the VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
802.1p	Selecting this option instructs the Switch to examine the 802.1p priority value of each packet header and use this as the, or part of the criterion for forwarding.
Ethernet Type	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.

Clicking **Create** on the previous **Add ACL Profile** window inserts a new Access Profile List entry in the **Access Profile List** window shown below. To add another Access Profile, click **Add ACL Profile**. To delete a profile click the corresponding **Delete** button, to view the specific configurations for an entry click the **Show Details** button. To add a rule to the Access Profile entry, click the **Add/View Rules** button.

Figure 6 - 4. Access Profile List window for Ethernet example

To view the configurations for a previously configured entry, click on the corresponding **Show Details** button, which will display the following window:

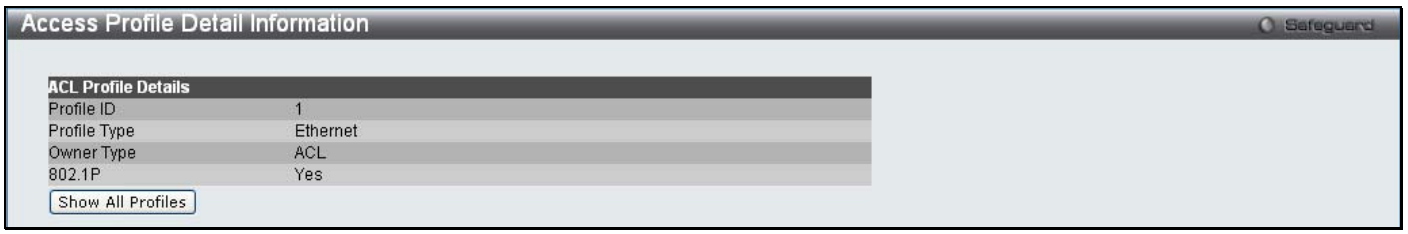


Figure 6 - 5. Access Profile Detail Information window for Ethernet example

To return to the **Access Profile List** window, click **Show All Profiles**. To add a rule to a previously configured entry click on the corresponding **Add/View Rules**. The following window is displayed:

Figure 6 - 6. initial Access Rule List window

Click **Add Rule**, which will reveal the following window:

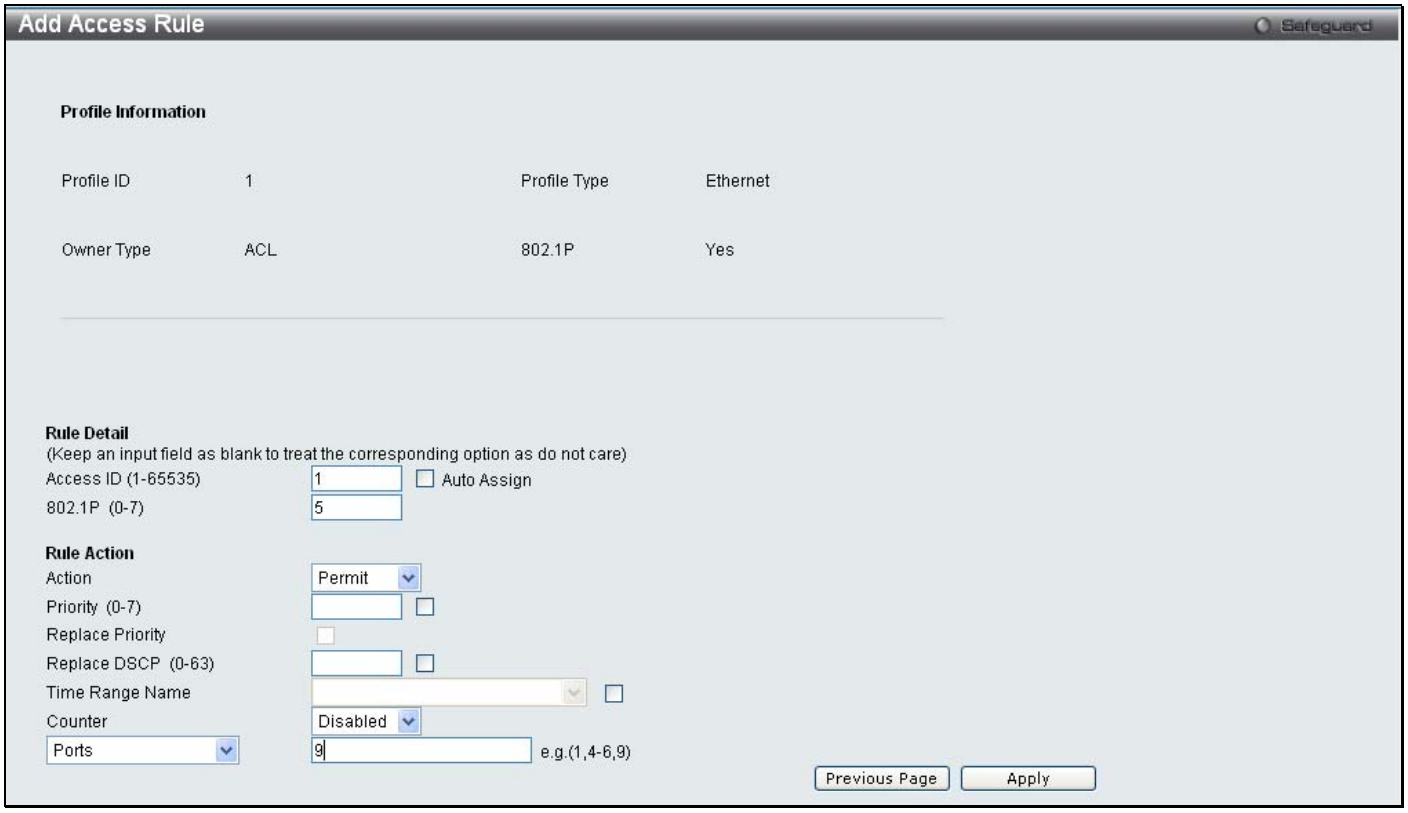


Figure 6 - 7. Add Access Rule window for Ethernet example

To set the Access Rule for Ethernet, adjust the following parameters and click **Apply**.

Parameter	Description
Access ID (1-65535)	Type in a unique identifier number for this access. This value can be set from *1* to *65535*. Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
VLAN Name	Selecting this option instructs the Switch to examine the VLAN part of each packet header and use this as the, or part of the, criterion for forwarding
VLAN ID (1-4094)	Mask ____ (0-FFF) – Specifies a VLAN ID.
VLAN ID	Allows the entry of a VLAN ID for a previously configured VLAN.
Source MAC Address	Specifies a MAC address mask for the source MAC address.
Source MAC Mask	Specifies a MAC address mask for the source MAC address. This mask is entered in a hexadecimal format.
Destination MAC Address	Specifies a MAC address for the destination MAC address.
Destination MAC Mask	Specifies a MAC address mask for the destination MAC address.
802.1p (0-7)	Enter a value from *0* to *7* to specify that the access profile will apply only to packets with this 802.1p priority value.
Ethernet Type (0-FFFF)	Enter a value that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value in the packet header.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify the packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined

	in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Priority (0-7)	Enter a priority value if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace Priority	Enter a replace priority manually if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Specifies whether counter feature will be enabled or disabled. This is optional, the default is disabled.
Ports	Enter a range of ports to be configured.

Click **Apply** to display the following **Access Rule List** window:

Figure 6 - 8. Access Rule List window for Ethernet example

To view the configurations for previously configured rules, click on the corresponding **Show Details** button, which will display the following **Access Rule Detail Information** window:

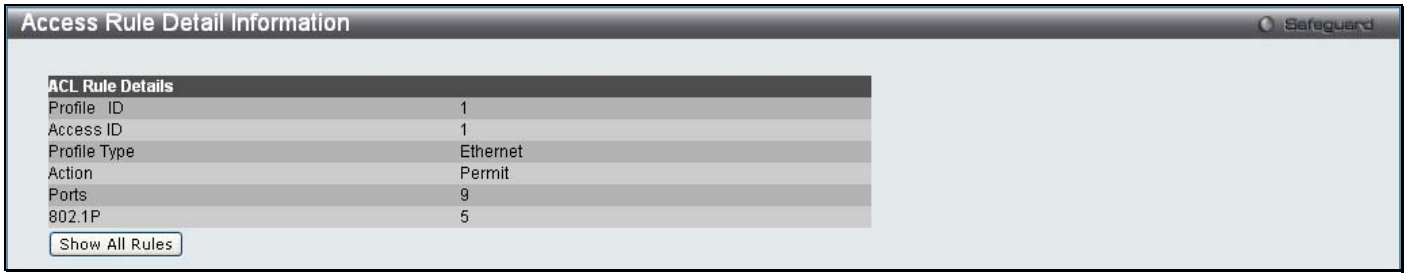


Figure 6 - 9. Access Rule Detail Information window for Ethernet example

To create an IPv4 ACL, click **Add ACL Profile** in the **Access Profile List** window and then use the drop-down menu to select a Profile ID between *1* and *512*, click the IPv4 ACL radio button, and then use the drop-down menu to select a protocol *ICMP*, *IGMP*, *TCP*, *UDP*, or *Protocol ID*. Click **Select** and the following window will appear (this window will vary depending on whether *ICMP*, *IGMP*, *TCP*, *UDP*, or *Protocol ID* has been selected):

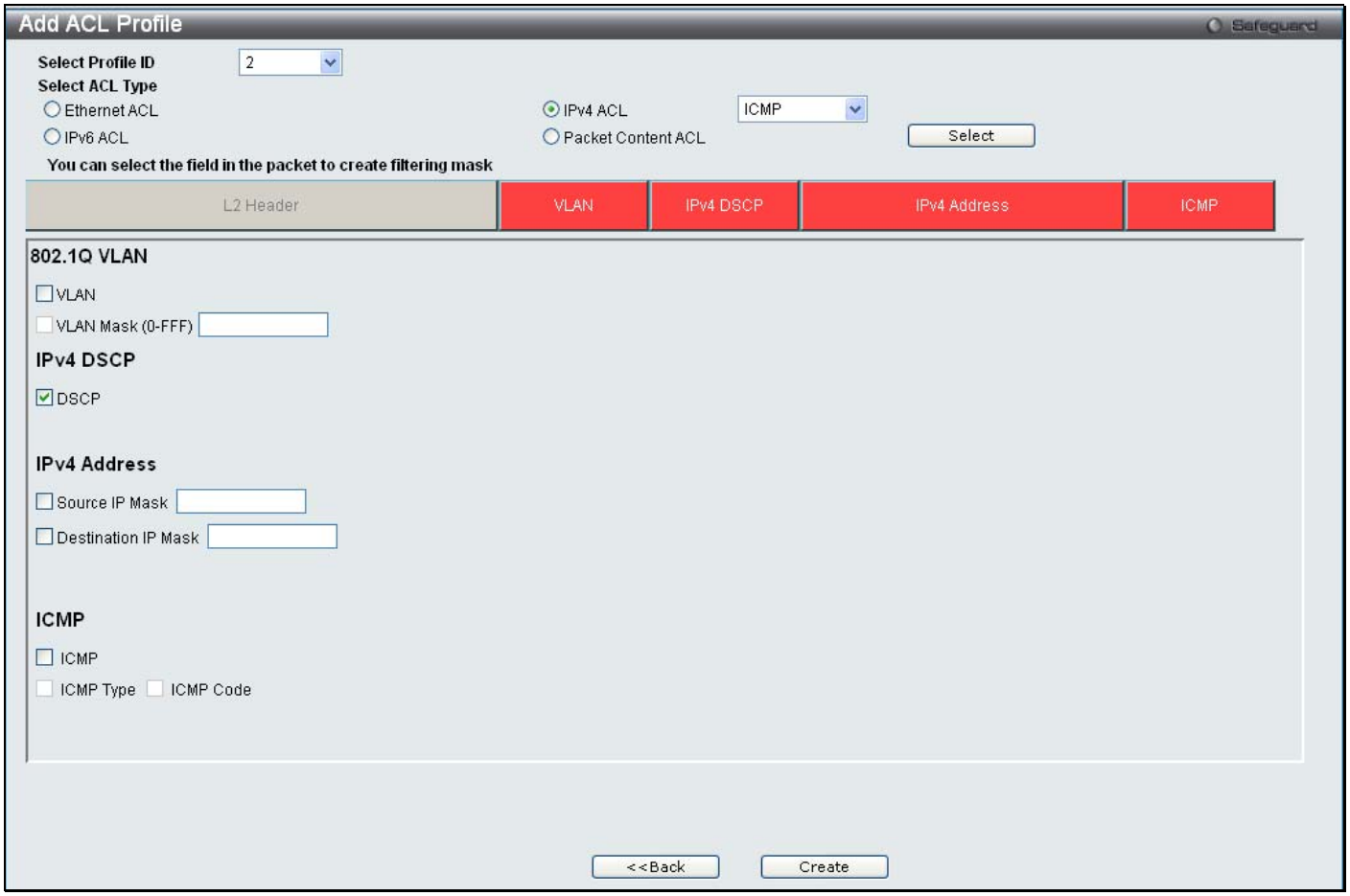


Figure 6 - 10. Add ACL Profile window for IPv4 example

Click on the boxes near the top of the window, which will then turn red and reveal parameters for configuration. To create a new entry, enter the appropriate information and click **Create**. To return to the **Access Profile List** window, click **<<Back**.

The following parameters can be set for IPv4:

Parameter	Description
VLAN	Selecting this option instructs the Switch to examine the VLAN part of each packet header and use this as the, or part of the, criterion for forwarding.
IPv4 DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.
IPv4 Address	Tick either Source IP Mask and enter the IPv4 source address mask or Destination IP Mask and enter the IPV4 destination address mask.
ICMP	Tick ICMP to specify that the Switch will examine the Internet Control Message Protocol (ICMP) field within each packet. Tick ICMP Type to specify that the access profile will apply to this ICMP type value. Tick ICMP Code to specify that the access profile will apply to this ICMP code value.
IGMP	Tick IGMP to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header. Tick IGMP Type to further specify that the access profile will apply an IGMP type value.
TCP	Tick TCP to use the TCP port number contained in an incoming packet as the forwarding criterion. Ticking TCP requires specifying a source port mask and/or a destination port mask. The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits

	within the packets, by checking the boxes corresponding to the flag bits of the TCP field. Source Port Mask (0-FFFF) – Tick and specify a TCP port mask for the source port to filter, in hex form (hex 0x0-0xffff). Destination Port Mask (0-FFFF) – Tick and specify a TCP port mask for the destination port to filter, in hex form (hex 0x0-0xffff). TCP Flag Bits – Tick URG (urgent), ACK (acknowledgement), PSH (push), RST (reset), SYN (synchronize), FIN (finish), or Check All to filter certain flag bits within the packets.
UDP	Tick UDP to use the UDP port number contained in an incoming packet as the forwarding criterion. Ticking UDP requires specifying a source port mask and/or a destination port mask. Source Port Mask – Tick and specify a TCP port mask for the source port to filter, in hex form (hex 0x0-0xffff). Destination Port Mask – Tick and specify a TCP port mask for the destination port to filter, in hex form (hex 0x0-0xffff).
Protocol ID	Tick Protocol ID Mask and enter a value defining the protocol ID in the packet header to mask. Protocol ID Mask (0-FF) – Tick and enter a value defining the mask options behind the IP header.

Click **Apply** to implement changes made.

Click **Create** to view the new Access Profile List entry in the **Access Profile List** window shown below. To add another Access Profile click **Add ACL Profile**. To delete a profile click the corresponding **Delete** button, to view the specific configurations for an entry click the **Show Details** button. To add a rule to the Access Profile entry, click the **Add/View Rules** button.

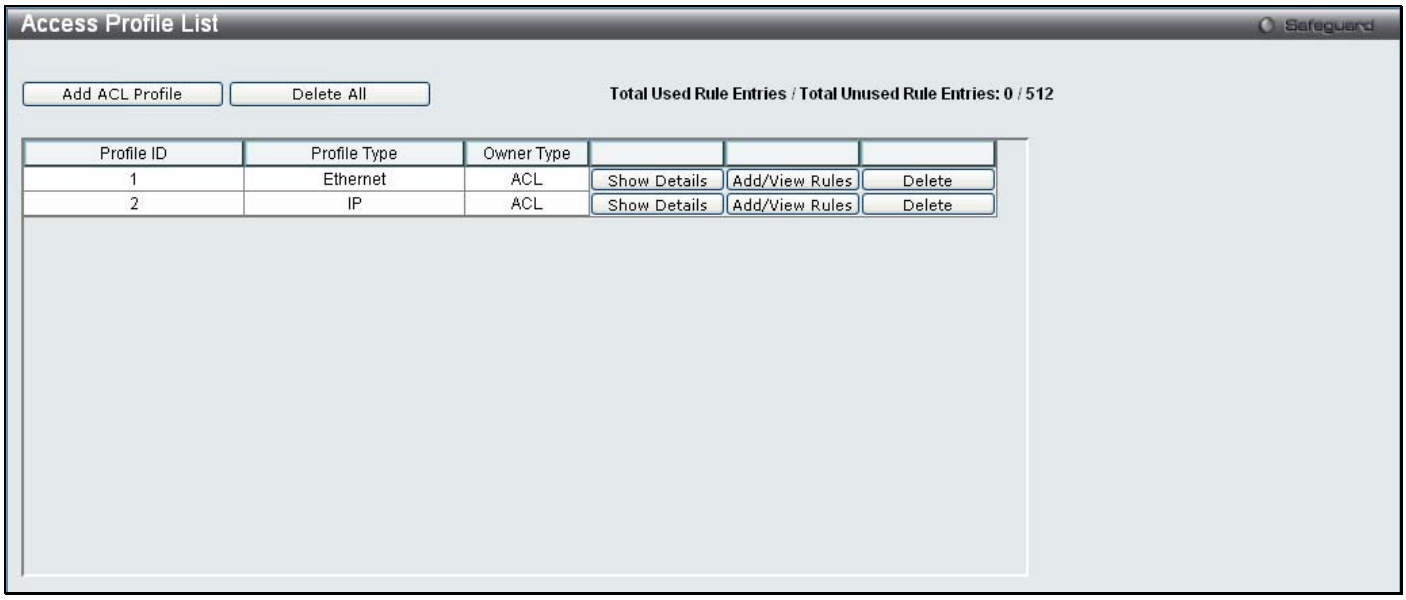


Figure 6 - 11. Access Profile List window for IPv4 example

To view the configurations for a previously configured entry, click on the corresponding **Show Details** button, which will display the following window:

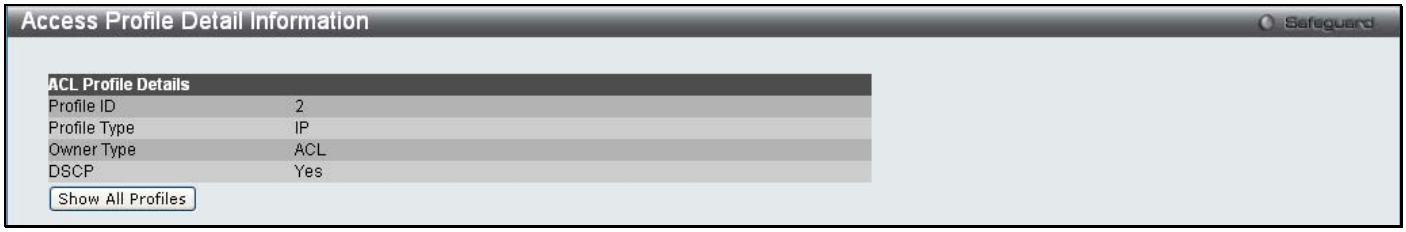


Figure 6 - 12. Access Profile Detail Information window for IPv4 example

To return to the **Access Profile List** window, click **Show All Profiles**. To add a rule to a previously configured entry, click on the corresponding **Add/View Rules** button, and then click **Add Rule** on the **Access Rule List** window, which will reveal the following window:

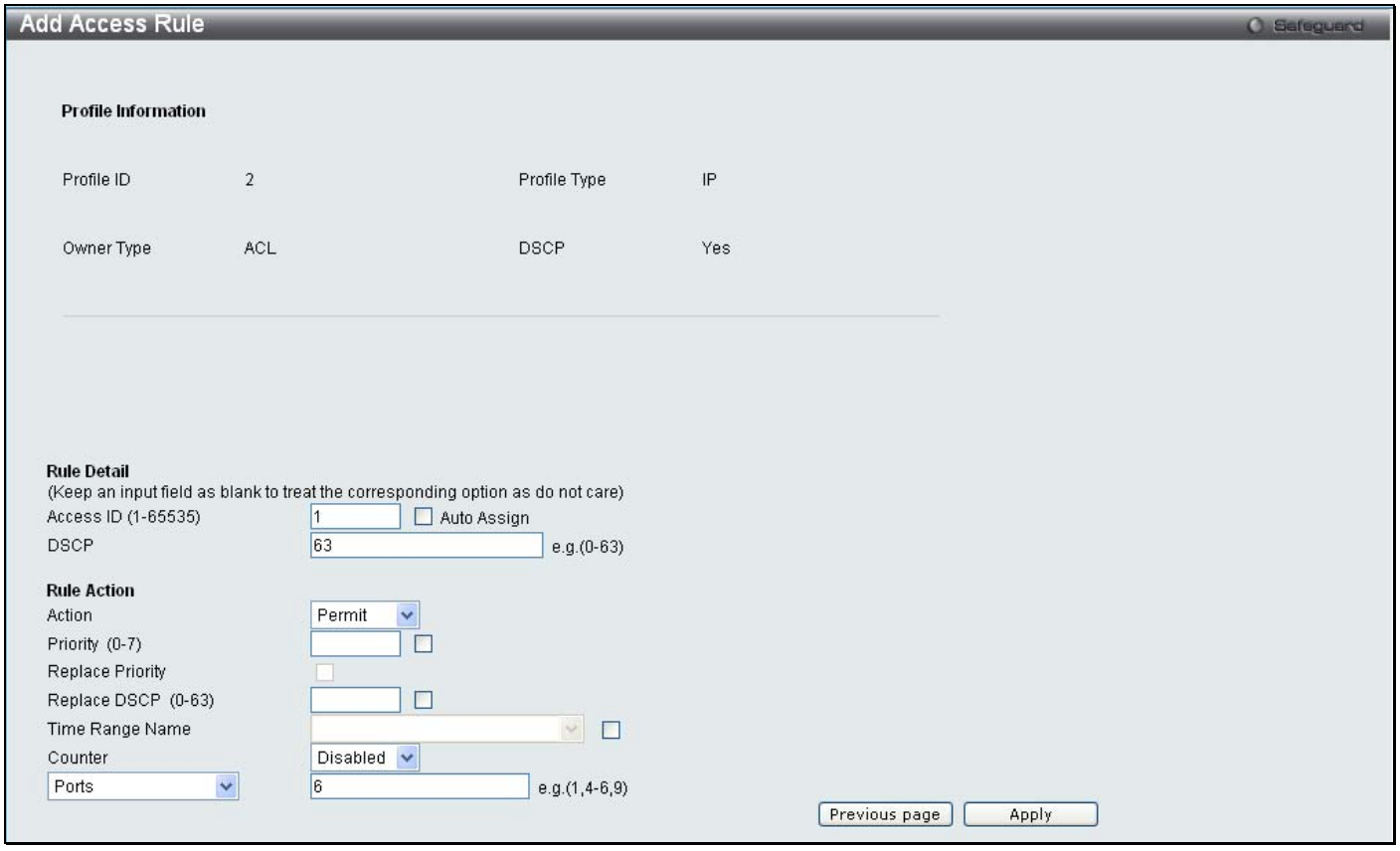


Figure 6 - 13. Add Access Rule window for IPv4 example

The following parameters may be configured for the IP (IPv4) filter:

Parameter	Description
Access ID (1-65535)	Type in a unique identifier number for this access. This value can be set from *1* to *65535*.
VLAN Name	Specifies a VLAN name.
VLAN ID (1-4094)	Mask ____ (0-FFF) – Specifies a VLAN ID.
Source IP Address	Specifies an IP address for the source IP address.
Source IP Mask	Specifies an IP address mask for the source IP address.
Destination IP Address	Specifies an IP address for the destination IP address.
Destination IP Mask	Specifies a destination IP address mask for the destination IP address.
DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the criteria, or part of the criterion for forwarding.
ICMP	Select *ICMP* to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header. ICMP Type - Specifies that the Switch will examine each frame's ICMP Type field.

	ICMP Code - Specifies that the Switch will examine each frame's ICMP Code field.
IGMP	Type ____ e.g. (0-255) - Specifies that the Switch will examine each frame's IGMP Type field.
TCP	Source Port - Specifies a TCP port for the source port. Mask (0-FFFF) - Specifies a TCP port mask for the source port. Destination Port - Specifies a TCP port for the destination port. Mask (0-FFFF) - Specifies a TCP port mask for the destination port. Flag Bits - Enter the appropriate flag mask parameter. All incoming packets have TCP port numbers contained in them as the forwarding criterion. These numbers have flag bits associated with them which are parts of a packet that determine what to do with the packet. The user may deny packets by denying certain flag bits within the packets. URG/ACK/PSH/RST/SYN/FIN – Choose among *urg* (urgent), *ack* (acknowledgement), *psh* (push), *rst* (reset), *syn* (synchronize) and *fin* (finish)
UDP	Source Port - Specifies that the Switch will examine each frame's Universal Datagram Protocol (UDP) field for the source port. Mask (0-FFFF) - Specifies a UDP port mask for the destination port. Destination Port - Specifies a UDP port for the destination port. Mask (0-FFFF) - Specifies a UDP port mask for the destination port.
Protocol ID	Protocol ID ___ e.g. (0-255) - Specifies that the Switch will examine the protocol field in each packet and if this field contains the value entered here, apply the following rules.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify the packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Priority (0-7)	Enter a priority value if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.
Replace Priority	Enter a replace priority manually if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Enable or disable the counter settings.
Ports	Enter a range of ports to be configured.

Click **Apply** to display the following **Access Rule List** window:

Figure 6 - 14. Access Rule List window for IPv4 example

To view the configurations for a previously configured rule, click on the corresponding **Show Details** button, which will display the following **Access Rule Detail Information** window:

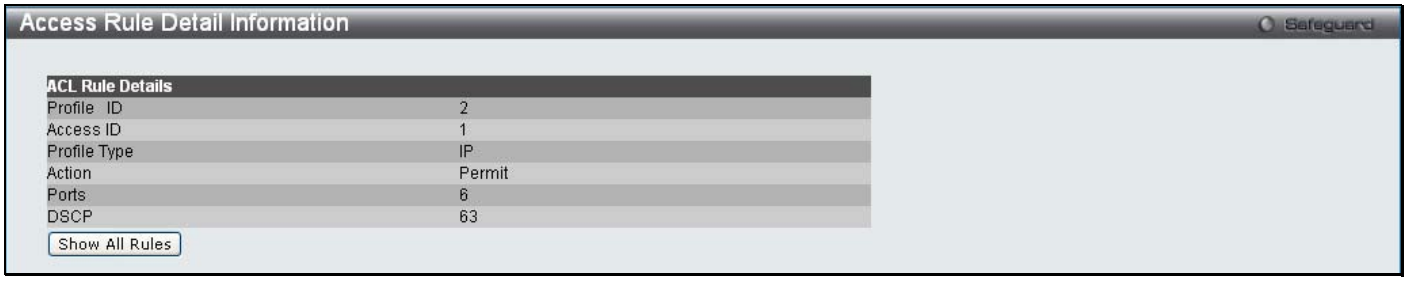


Figure 6 - 15. Access Rule Detail Information window for IPv4 example

To create an IPv6 ACL, click **Add ACL Profile** in the **Access Profile List** window and then use the drop-down menu to select a Profile ID between *1* and *512*, click the IPv6 ACL radio button, and then use the drop-down menu to select a protocol *TCP* or *UDP*. Click **Select** and the following window will appear (this window will vary depending on whether *TCP* or *UDP* has been selected):

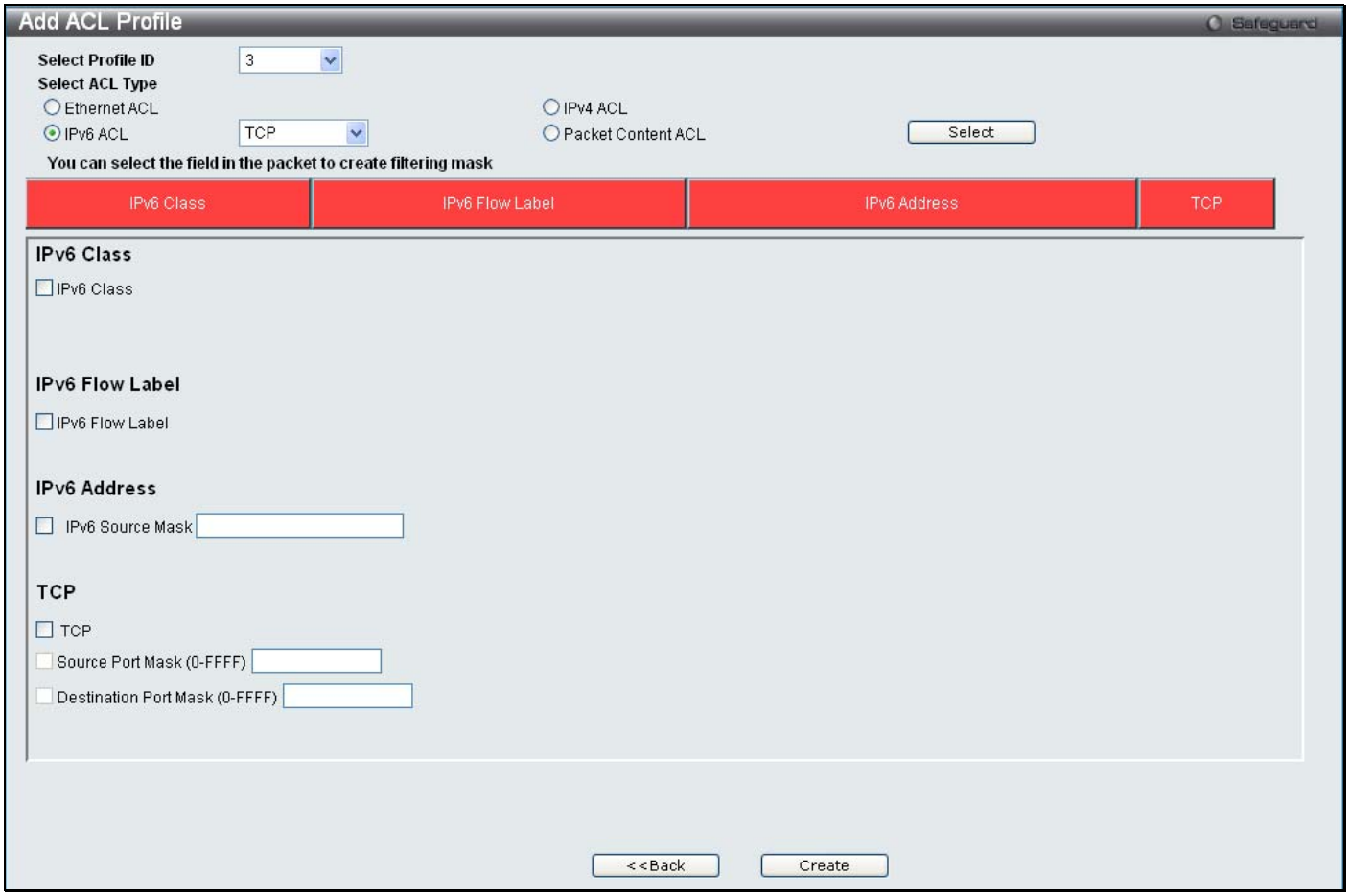


Figure 6 - 16. Add ACL Profile window for IPv6 example

Click on the boxes at the top of the table, which will then turn red and reveal parameters for configuration. To create a new entry enter the correct information and click **Create**. To return to the **Access Profile List** window, click **<<Back**.

The following parameters can be set for IPv6:

Parameter	Description
IPv6 Class	Ticking this check box will instruct the Switch to examine the class field of the IPv6 header. The class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4.

IPv6 Flow Label	Ticking this check box will instruct the Switch to examine the flow label field of the IPv6 header. The flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
IPv6 Address	Ticking this check box will instruct the Switch to examine the IPv6 Source Address.
IPv6 TCP	Ticking this check box will specify that the rule applies to TCP traffic. The user can tick and enter a specific TCP Source Port Mask or TCP Destination Port Mask.
IPv6 UDP	Ticking this check box will specify that the rule applies to UDP traffic. The user can tick and enter a specific UDP Source Port Mask or UDP Destination Port Mask.

Click **Apply** to implement changes made.

Click **Create** to view the new Access Profile List entry in the **Access Profile List** window shown below. To add another Access Profile, click **Add ACL Profile**. To delete a profile click the corresponding **Delete** button. To view the specific configurations for an entry click, the **Show Details** button. To add a rule to the Access Profile entry, click the **Add/View Rules** button.

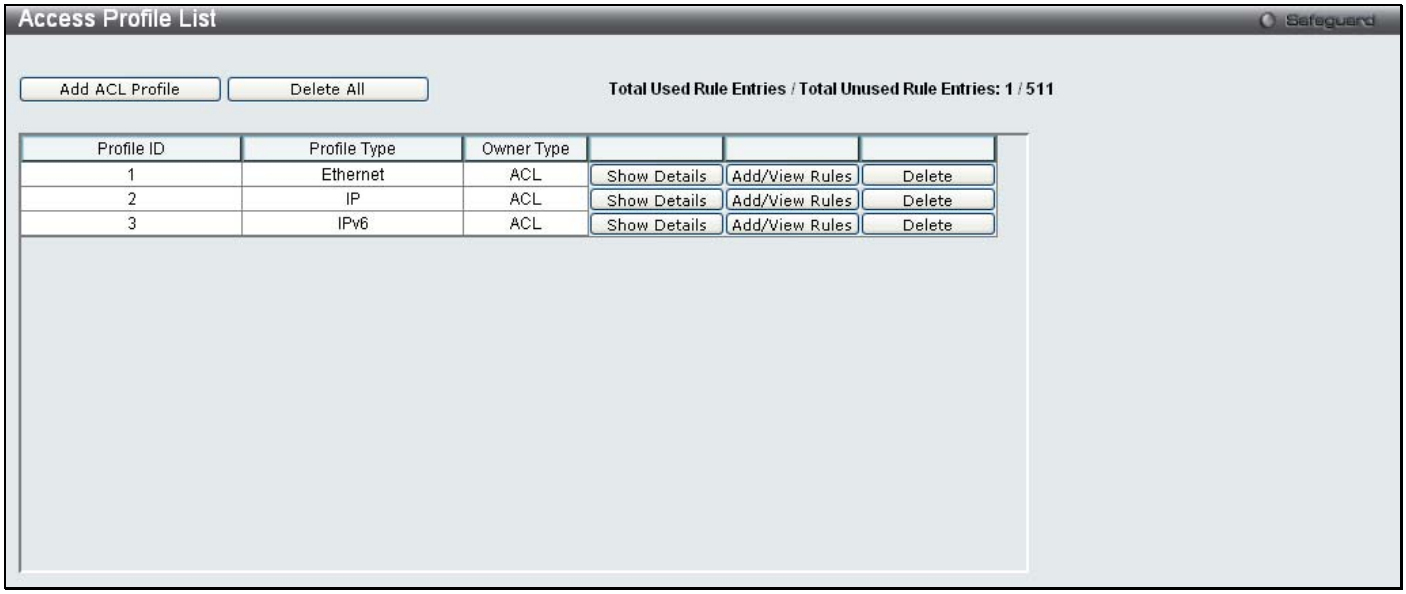


Figure 6 - 17. Access Profile List window for IPv6 example

To view the configurations for a previously configured entry, click on the corresponding **Show Details** button, which will display the following window:

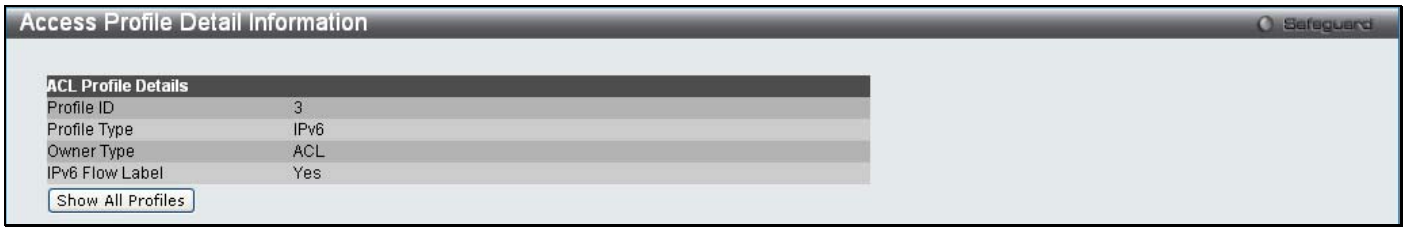


Figure 6 - 18. Access Profile Detail Information window for IPv6 example

To return to the **Access Profile Lis**t window, click **Show All Profiles**. To add a rule to a previously configured entry, click on the corresponding **Add/View Rules** button and then click **Add Rule** on the **Access Rule List** window, which will reveal the following window:

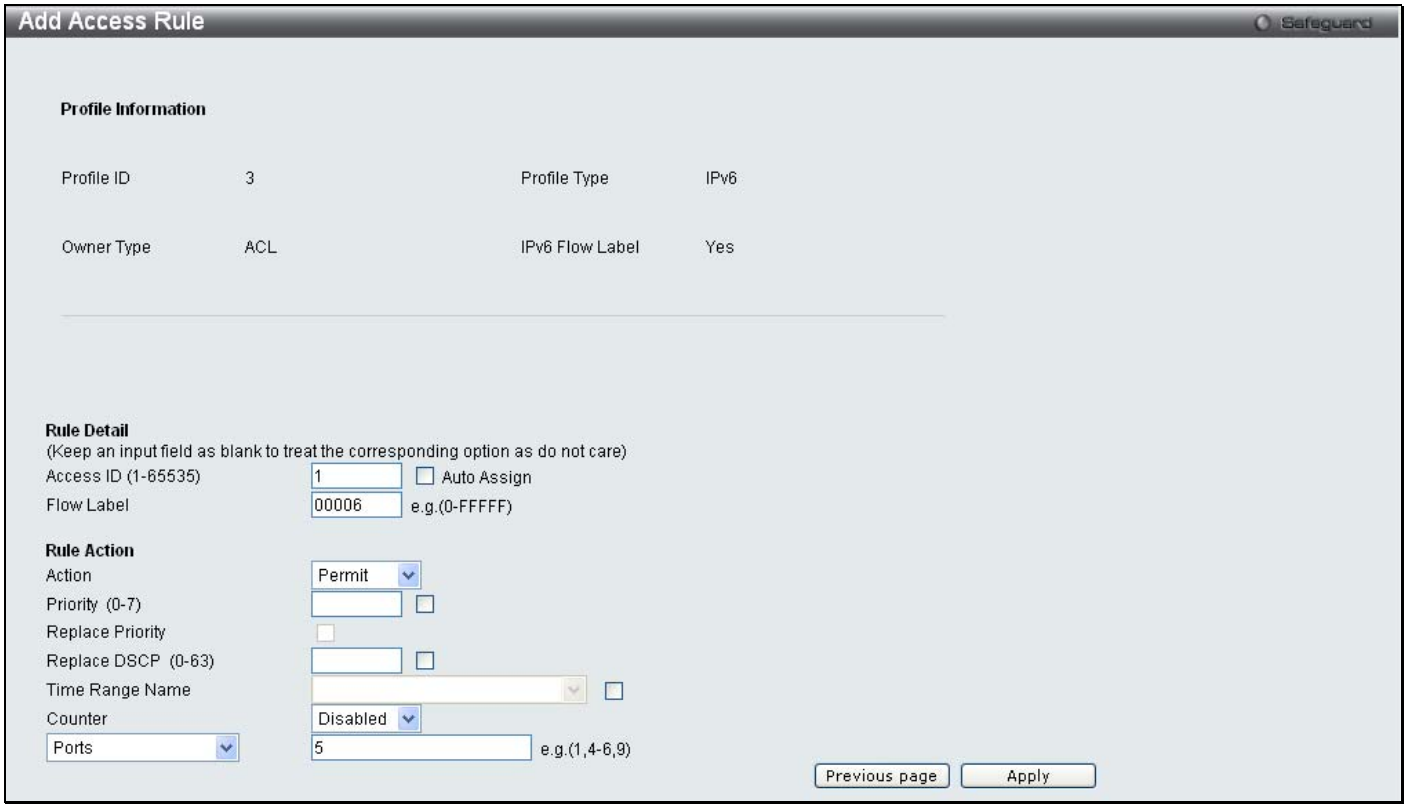


Figure 6 - 19. Add Access Rule window for IPv6 example

The following parameters may be configured for IPv6:

Parameter	Description
Access ID (1-65535)	Type in a unique identifier number for this access. This value can be set from *1* to *65535*. Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Class	Entering a class will instruct the Switch to examine the *class* field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4.
Flow Label	Specifies the IPv6 Flow Label. Enter a value between *0* – *FFFFF*.
IPv6 Source Address	Specifies an IPv6 address for the IPv6 source address.
IPv6 Source Mask	Specifies an IPv6 source submask. The device only supports filtering of the last 44 bits (LSB) of the source IPv6 address.
TCP	Source Port - Specifies an IPv6 L4 TCP source port submask. Destination Port - Specifies an IPv6 L4 TCP destination port submask.
UDP	Source Port - Specifies an IPv6 L4 UDP source port submask. Destination Port - Specifies an IPv6 L4 UDP destination port submask.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify the packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Priority (0-7)	Enter a priority value if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the

	Switch.
Replace Priority	Enter a replace priority manually if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Enable or disable the counter settings.
Ports	Enter a range of ports to be configured.

Click **Apply** to display the following **Access Rule List** window:

Figure 6 - 20. Access Rule List window for IPv6 example

To view the configurations for a previously configured rule, click on the corresponding **Show Details** button, which will display the following **Access Rule Detail Information** window:

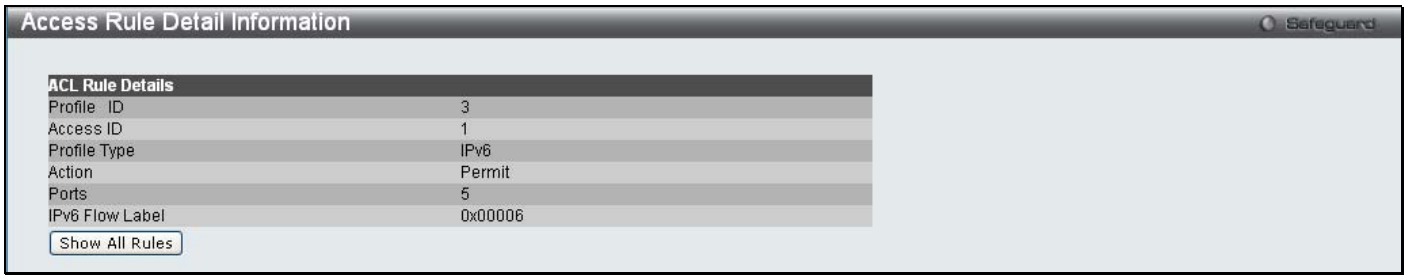


Figure 6 - 21. Access Rule Detail Information window for IPv6 example

To create a Packet Content ACL, click **Add ACL Profile** in the **Access Profile List** window and then use the drop-down menu to select a Profile ID between *1* and *512* and click the Packet Content ACL radio button. Click **Select** and the following window will appear:

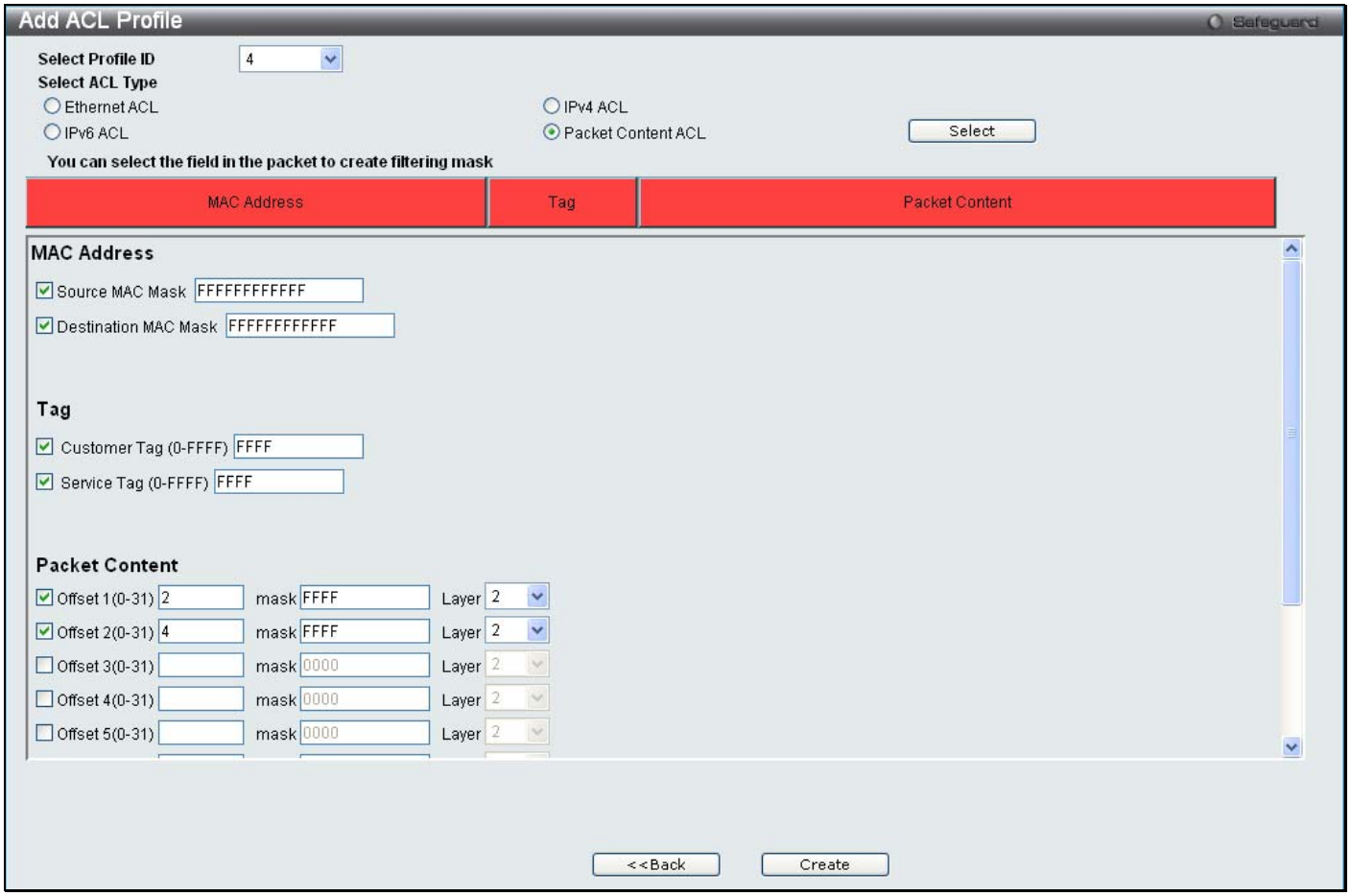


Figure 6 - 22. Add ACL Profile window for Packet Content example

Click on the boxes at the top of the table, which will then turn red and reveal parameters for configuration. To create a new entry enter the correct information and click **Create**. To return to the **Access Profile List** window, click **<<Back**.

The following parameters can be set for Packet Content:

Parameter	Description
MAC Address	Tick either Source MAC Mask and enter the MAC source address mask or Destination MAC Mask and enter the MAC destination address mask.
Tag	Tick Customer Tag (0-FFFF) and enter the appropriate customer tag, in hex form (hex 0x0-0xffff), and/or Service Tag (0-FFFF) and enter the appropriate service tag, in hex form (hex 0x0-0xffff).
Packet Content	Allows users to examine up to eleven specified offset packet content chunks within a packet at one time and specifies the frame content offset, mask, and layer. There are eleven packet content chunk offsets that can be configured. A packet content chunk mask presents two bytes. Up to eleven packet content offset chunks can be selected: Offset 1 (0-31) _____mask_____Layer ___, Offset 2 (0-31) _____mask_____Layer ___, Offset 3 (0-31) _____mask_____Layer ___, Offset 4 (0-31) _____mask_____Layer ___, Offset 5 (0-31) _____mask_____Layer ___, Offset 6 (0-31) _____mask_____Layer ___, Offset 7 (0-31) _____mask_____Layer ___, Offset 8 (0-31) _____mask_____Layer ___, Offset 9 (0-31) _____mask_____Layer ___, Offset 10 (0-31) _____mask_____Layer ___, Offset 11 (0-31) _____mask_____Layer ___

	With this advanced unique Packet Content Mask (also known as Packet Content Access Control List - ACL), the D-Link xStack® switch family can effectively mitigate some network attacks like the common ARP Spoofing attack that is wide spread today. This is why the Packet Content ACL is able to inspect any specified content of a packet in different protocol layers.

Click **Apply** to implement changes made.

Click **Create** to view the new Access Profile List entry in the **Access Profile List** window shown below. To add another Access Profile, click **Add ACL Profile**. To delete a profile, click the corresponding **Delete** button. To view the specific configurations for an entry, click the **Show Details** button. To add a rule to the Access Profile entry, click the **Add/View Rules** button.

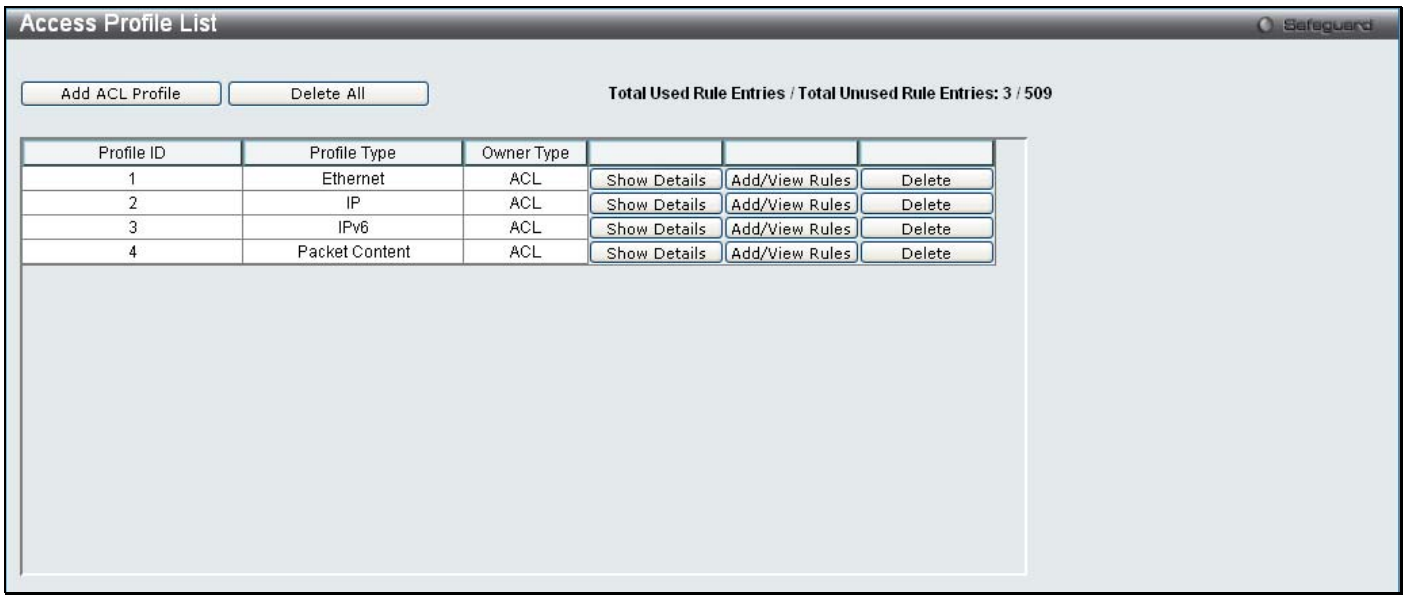


Figure 6 - 23. Access Profile List window for Packet Content example

To view the configurations for a previously configured entry, click on the corresponding **Show Details** button, which will display the following window:

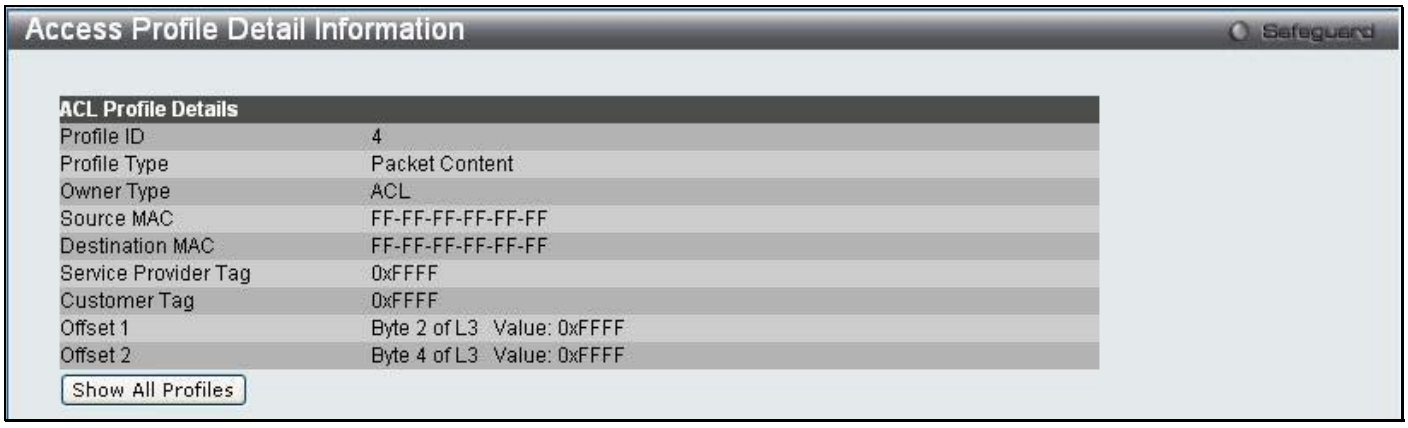


Figure 6 - 24. Access Profile Detail Information window for Packet Content example

To return to the **Access Profile List** window, click **Show All Profiles**. To add a rule to a previously configured entry, click on the corresponding **Add/View Rules** button and then **Add Rule**, which will reveal the following window:

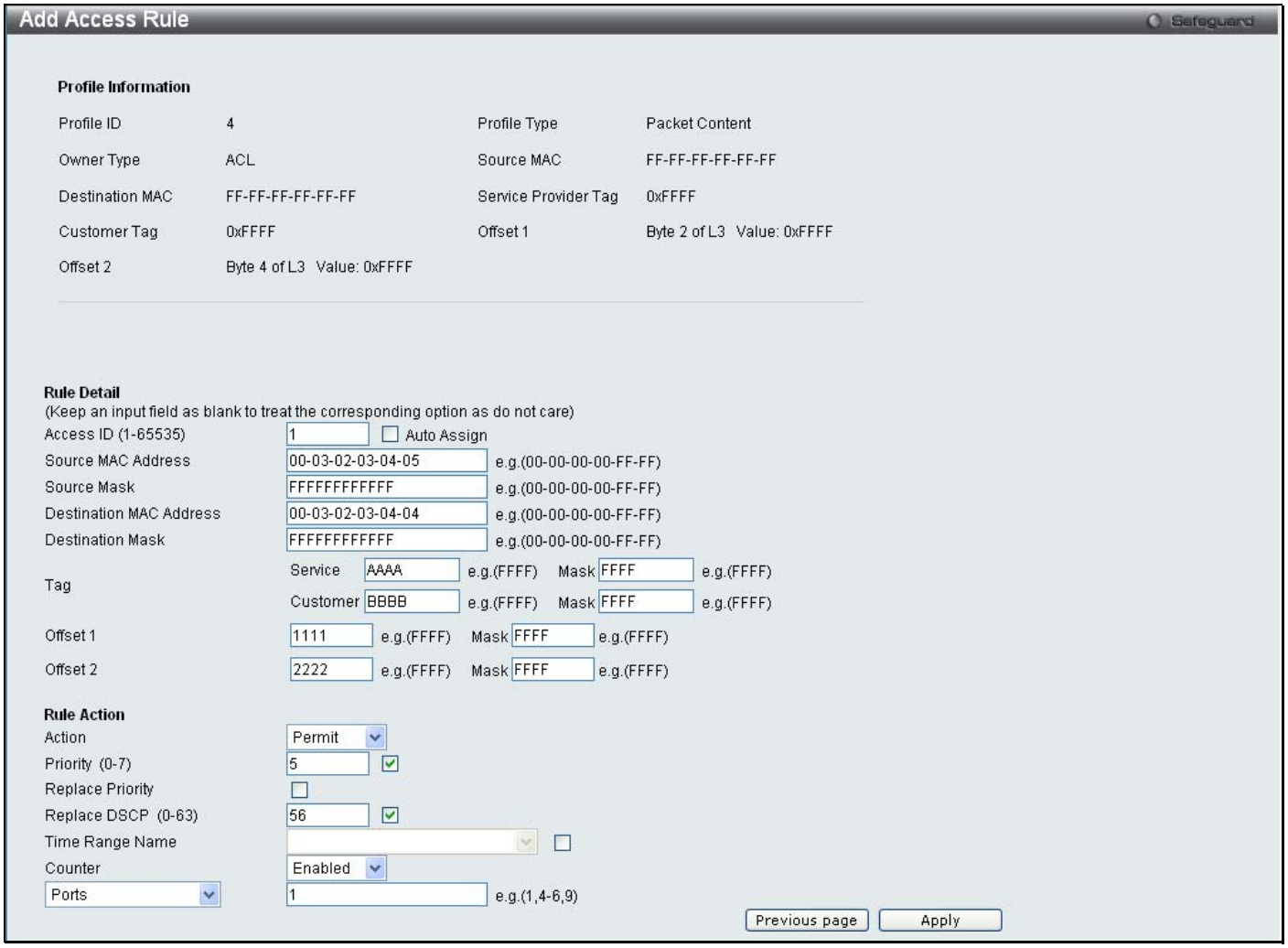

Add Access Rule
Safeguard
Profile Information
Profile ID 4
Profile Type Packet Content
Owner Type ACL
Source MAC FF-FF-FF-FF-FF-FF
Destination MAC FF-FF-FF-FF-FF-FF
Service Provider Tag 0xFFFF
Customer Tag 0xFFFF
Offset 1 Byte 2 of L3 Value: 0xFFFF
Offset 2 Byte 4 of L3 Value: 0xFFFF
Rule Detail
(Keep an input field as blank to treat the corresponding option as do not care)
Access ID (1-65535) 1 Auto Assign
Source MAC Address 00-03-02-03-04-05 e.g.(00-00-00-00-FF-FF)
Source Mask FFFFFFFFFFFF e.g.(00-00-00-00-FF-FF)
Destination MAC Address 00-03-02-03-04-04 e.g.(00-00-00-00-FF-FF)
Destination Mask FFFFFFFFFFFF e.g.(00-00-00-00-FF-FF)
Tag
Service AAAA e.g.(FFFF) Mask FFFF e.g.(FFFF)
Customer BBBB e.g.(FFFF) Mask FFFF e.g.(FFFF)
Offset 1 1111 e.g.(FFFF) Mask FFFF e.g.(FFFF)
Offset 2 2222 e.g.(FFFF) Mask FFFF e.g.(FFFF)
Rule Action
Action Permit
Priority (0-7) 5
Replace Priority
Replace DSCP (0-63) 56
Time Range Name
Counter Enabled
Ports 1 e.g.(1,4-6,9)
Previous page
Apply

Figure 6 - 25. Add Access Rule window for Packet Content example

The following parameters may be configured for the Packet Content filter:

Parameter	Description
Access ID (1-65535)	Type in a unique identifier number for this access. This value can be set from *1* to *65535*.
Source MAC Address	Specify the source MAC address of the packets that needed to be examined.
Source Mask	Specify a mask for the source MAC address. The filter is the result of the AND operation between this mask and the source MAC address.
Destination MAC Address	Specify the destination MAC address of the packets that need to be examined.
Destination Mask	Specify a mask for the destination MAC address. The filter is the result of the AND operation between this mask and the destination MAC address.
Tag	Specify the values for customer and service tags which need to be examined. The “mask” options can be used to mask the tag values. That is, the final filter is the result of the AND operation between the customer/service tag values and their corrersponding masks.
Offset	Specifies the 2-byte value of the chunk which needs to be examined. The mask option can be used to mask the 2-byte value of the chunk. The final filter is the result of the AND operation between the chunk value and the mask.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify the packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port

	must be set.
Priority (0-7)	Enter a priority value if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.
Replace DSCP	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Enable or disable the counter for this ACL rule.
Ports	Enter a range of ports to be configured.

Click **Apply** to display the following **Access Rule List** window:

Figure 6 - 26. Access Rule List window for Packet Content example

To view the configurations for a previously configured rule, click on the corresponding **Show Details** button, which will display the following **Access Rule Detail Information** window:

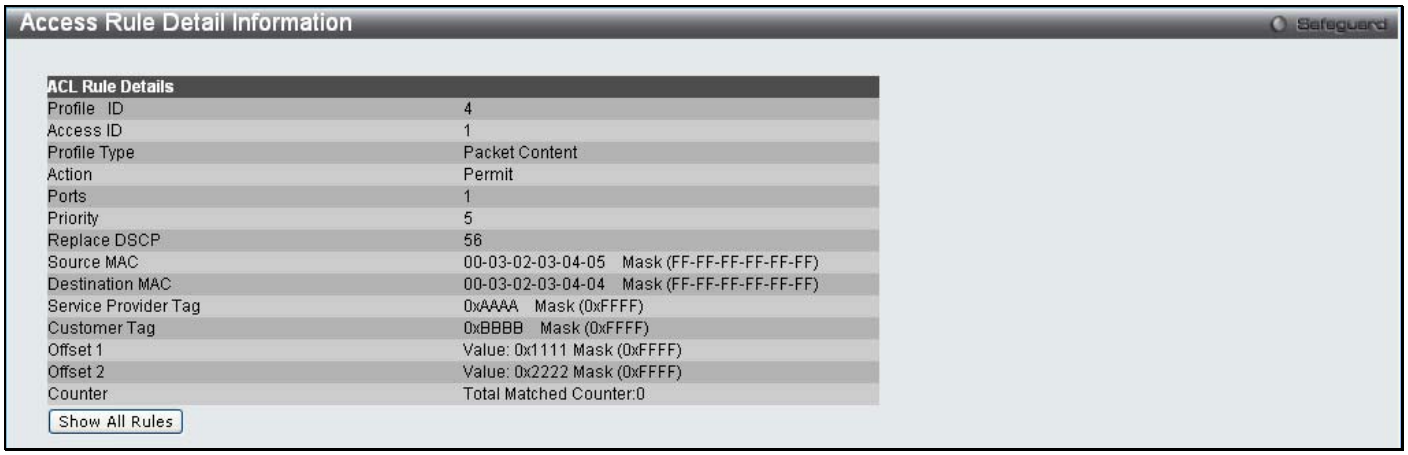


Figure 6 - 27. Access Rule Detail Information window for Packet Content example

NOTE: Address Resolution Protocol (ARP) is the standard for finding a host's hardware address (MAC Address). However, ARP is vulnerable as it can be easily spoofed and utilized to attack a LAN. For a more detailed explanation on how ARP works and how to employ D-Link's advanced unique Packet Content ACL to prevent ARP spoofing attack, please see Appendix B, at the end of this manual.

CPU Interface Filtering

Due to a chipset limitation and needed extra switch security, the Switch incorporates CPU Interface filtering. This added feature increases the running security of the Switch by enabling the user to create a list of access rules for packets destined for the Switch's CPU interface. Employed similarly to the Access Profile feature previously mentioned, CPU interface filtering examines Ethernet, IP and Packet Content Mask packet headers destined for the CPU and will either forward them or filter them, based on the user's implementation. As an added feature for the CPU Filtering, the Switch allows the CPU filtering mechanism to be enabled or disabled globally, permitting the user to create various lists of rules without immediately enabling them.

Creating an access profile for the CPU is divided into two basic parts. The first is to specify which part or parts of a frame the Switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the Switch will use to determine what to do with the frame. The entire process is described below.

CPU Access Profile List

In the following window, the user may globally enable or disable the CPU Interface Filtering State mechanism by using the radio buttons to change the running state.

To access this window, click **ACL > CPU Access Profile List**

Choose Enabled to enable CPU packets to be scrutinized by the Switch and Disabled to disallow this scrutiny.

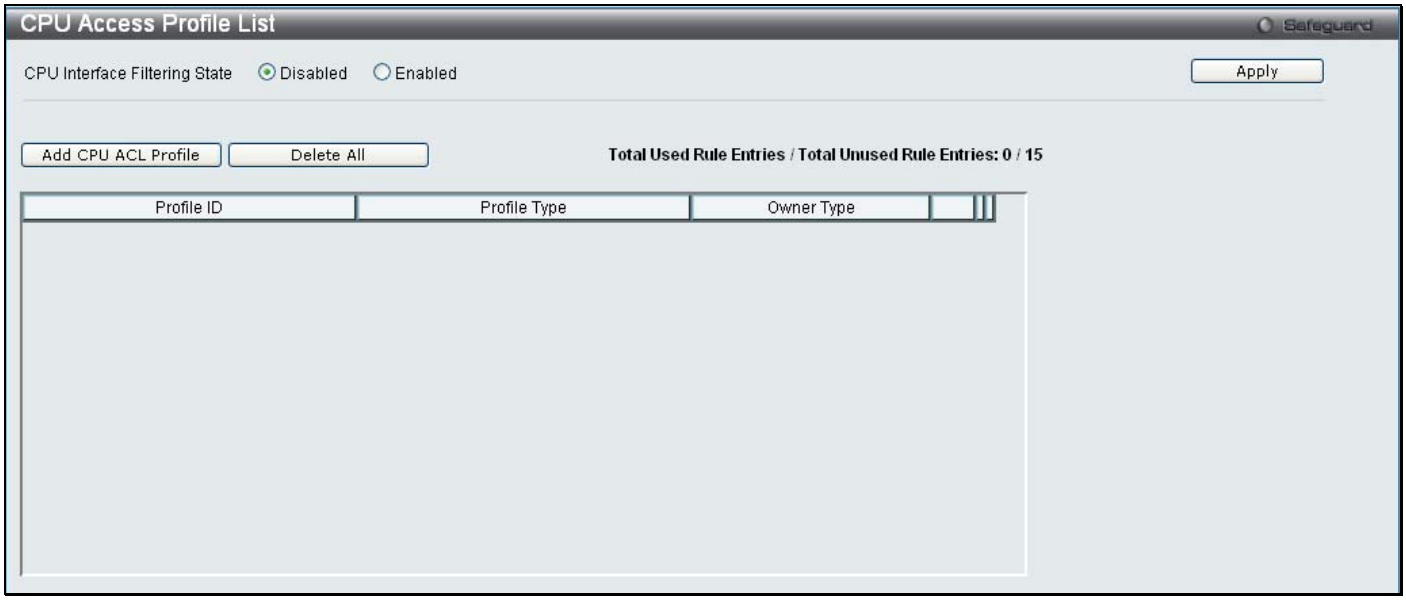


Figure 6 - 28. CPU Access Profile List window

This window displays the CPU Access Profile List entries created on the Switch. To view the configurations for an entry, click the corresponding **Show Details** button (once an entry has been created).

To add an entry to the **CPU Access Profile List** window, click the **Add CPU ACL Profile** button. This will open the **Add CPU ACL Profile** window. Click the **Select** button to see the window, as shown below. To remove all CPU Access Profile List entries, click the **Delete All** button.

The Switch supports four CPU Access Profile types: Ethernet (or MAC address-based) profile configuration, IP (IPv4) address-based profile configuration, IPv6 address-based profile configuration, and Packet Content Mask.

The window shown below is the **Add CPU ACL Profile** window for Ethernet:

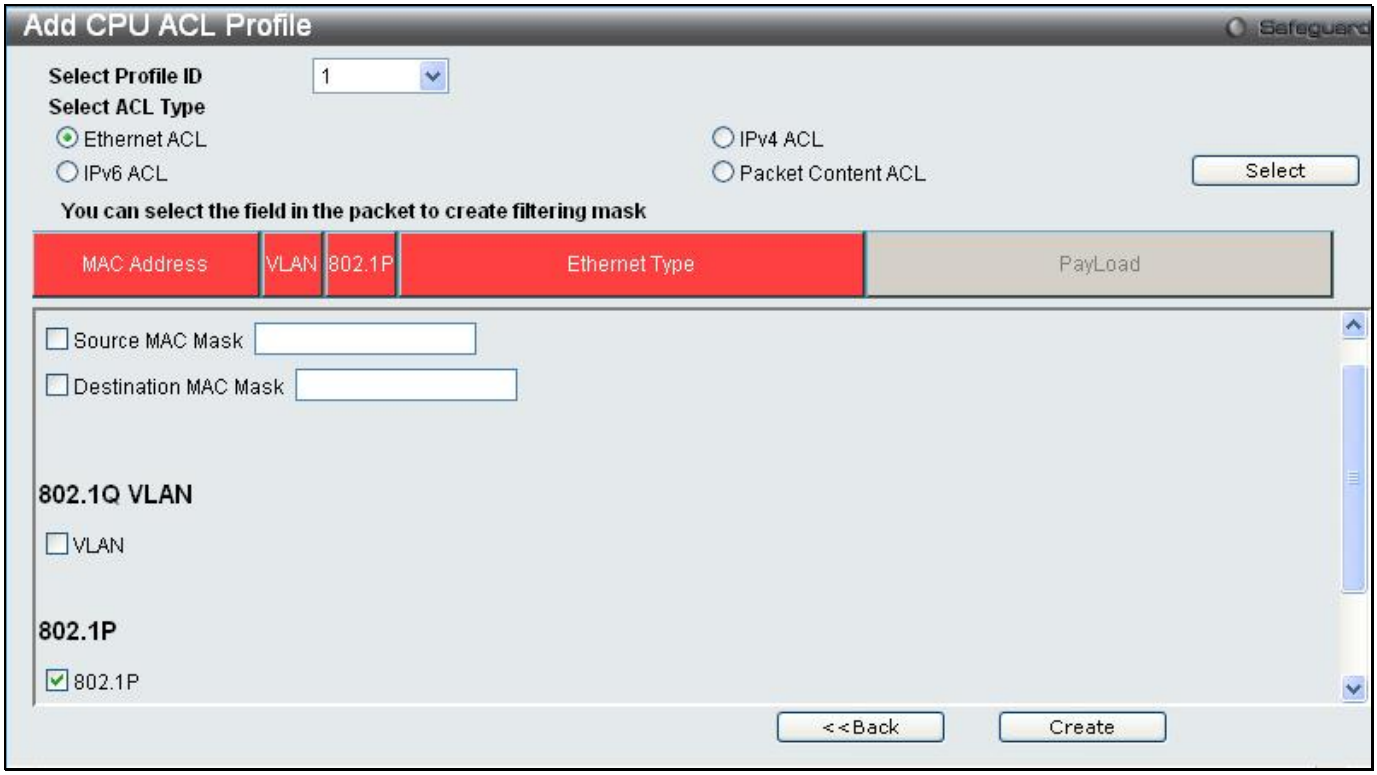


Figure 6 - 29. Add CPU ACL Profile window for Ethernet example

Parameter	Description
Select Profile ID (1-3)	Use the drop-down menu to select a unique identifier number for this profile set. This value can be set from *1* to *3*.
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6, or packet content mask. This will change the menu according to the requirements for the type of profile. Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header. Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header. Select Packet Content ACL to specify a mask to hide the content of the packet header.
MAC Address	Tick either Source MAC Mask and enter a source MAC address mask for the source MAC address or Destination MAC Mask and enter a destination MAC address mask for the destination MAC address.
802.1Q VLAN	Ticking this option instructs the Switch to examine the VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
802.1p	Ticking this option instructs the Switch to specify that the access profile will apply only to packets with this 802.1p priority value.
Ethernet Type	Ticking this option instructs the Switch to examine the Ethernet type value in each frame's header.

Click **Apply** to set this entry in the Switch's memory.

The following **CPU Access Profile List** window opens:

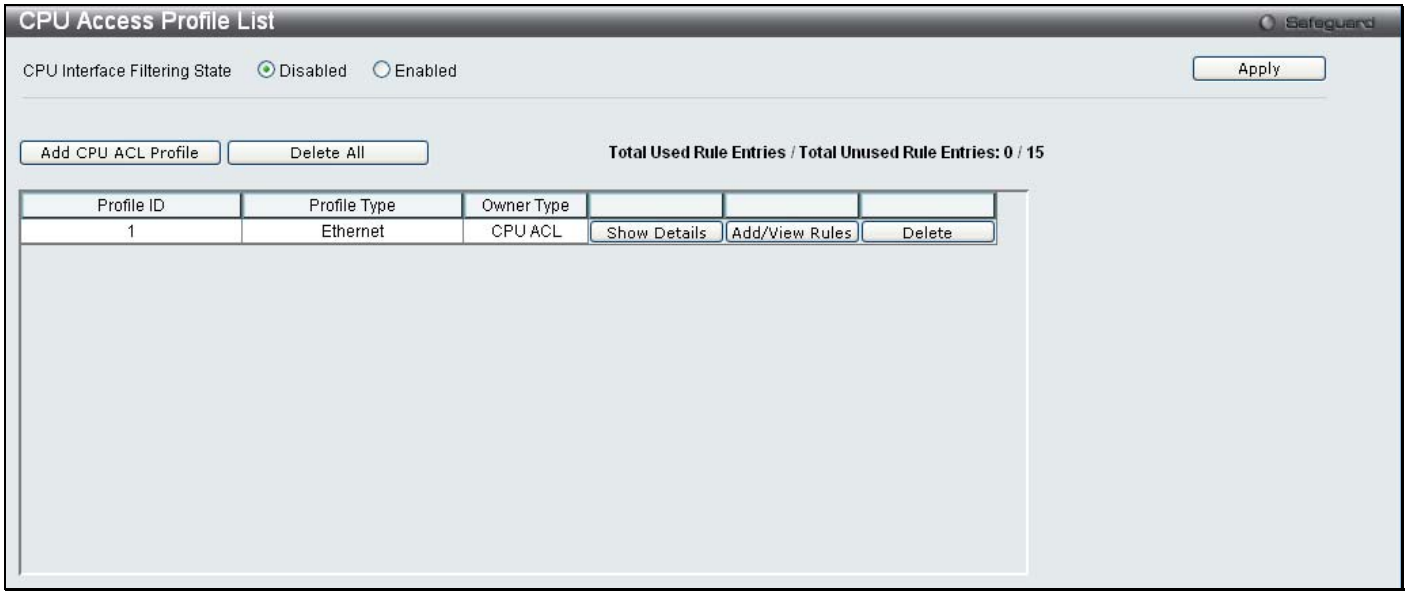


Figure 6 - 30. CPU Access Profile List window for Ethernet example

To view the settings of a previously correctly created profile, click the corresponding **Show Details** button on the following **CPU Access Profile List** window above. The following window opens:

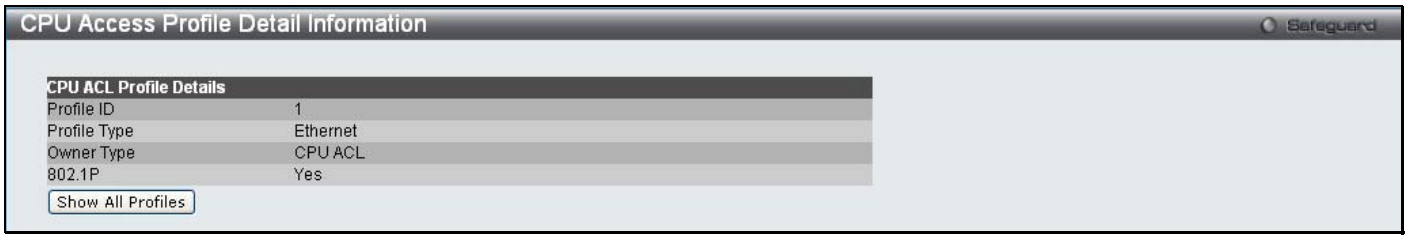


Figure 6 - 31. CPU Access Profile Detail Information window for Ethernet

To return to the **CPU Access Profile List** window, click **Show All Profiles**. To add a rule to a previously configured entry click on the corresponding **Add/View Rules**. The following window is displayed:

Figure 6 - 32. initial CPU Access Rule List window

Click **Add Rule**, which will reveal the following window:

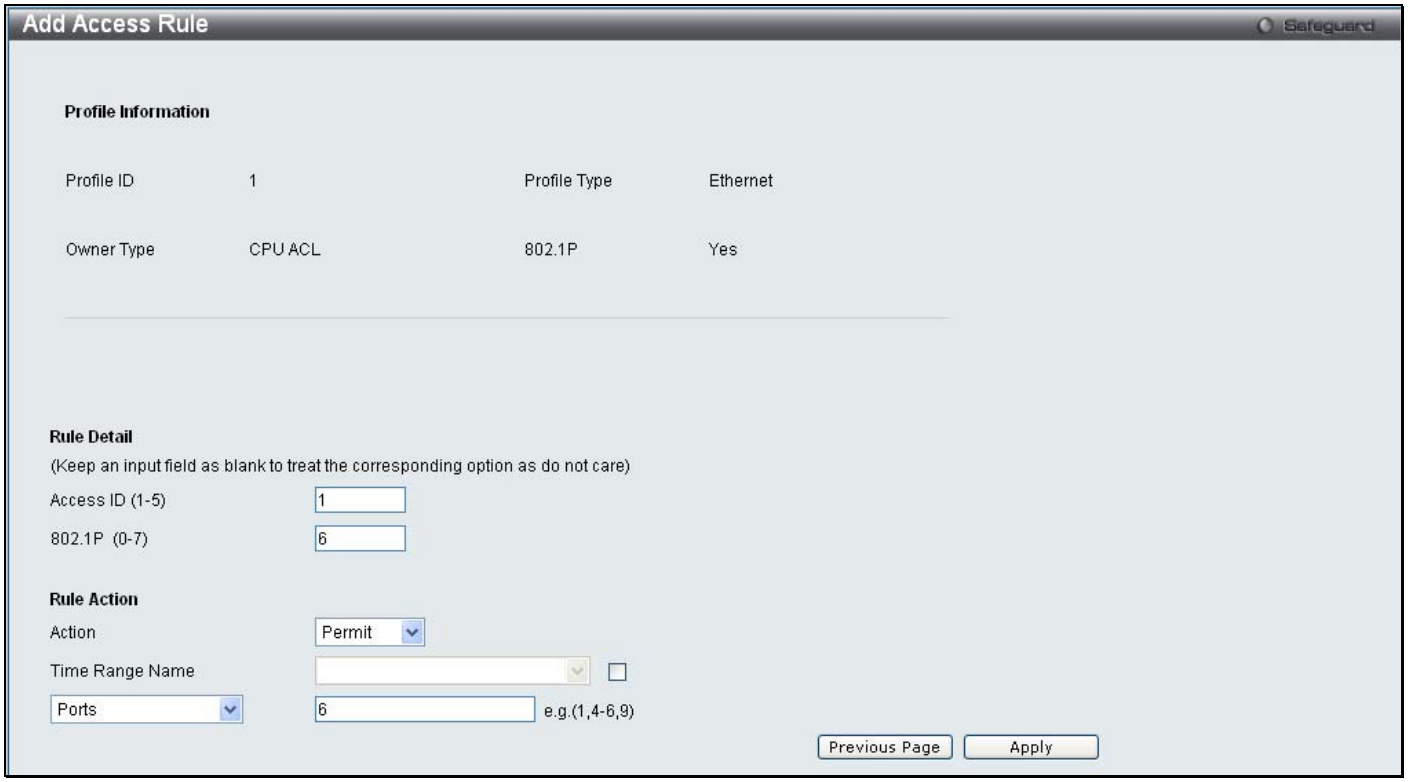


Figure 6 - 33. (CPU) Add Access Rule window for Ethernet example

To set the Access Rule for Ethernet, adjust the following parameters and click **Apply**.

Parameter	Description
Access ID (1-5)	Type in a unique identifier number for this access. This value can be set from *1* to *5*.
802.1p (0-7)	Enter a value from *0* to *7* to specify that the access profile will apply only to packets with this 802.1p priority value.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify the packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Ports	Enter a range of ports to be configured.

Click **Apply** to display the following **Access Rule List** window:

Figure 6 - 34. CPU Access Rule List window for Ethernet example

To view the configurations for previously configured rules, click on the corresponding **Show Details** button, which will display the following **CPU Access Rule Detail Information** window:

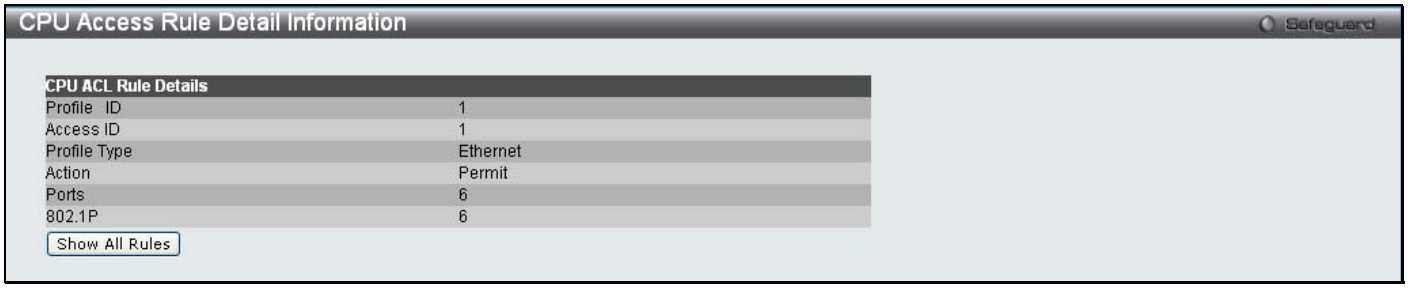


Figure 6 - 35. CPU Access Rule Detail Information window for Ethernet example

To create an IPv4 ACL, click **Add CPU ACL Profile** in the **CPU Access Profile List** window. This will open the **Add CPU ACL Profile** window. Use the drop-down menu to select a Profile ID between *1* and *3*, click the IPv4 ACL radio button, and then use the drop-down menu to select a protocol *ICMP*, *IGMP*, *TCP*, *UDP*, or *Protocol ID*. Click **Select** and the following window will appear (this window will vary depending on whether *ICMP*, *IGMP*, *TCP*, *UDP*, or *Protocol ID* has been selected):

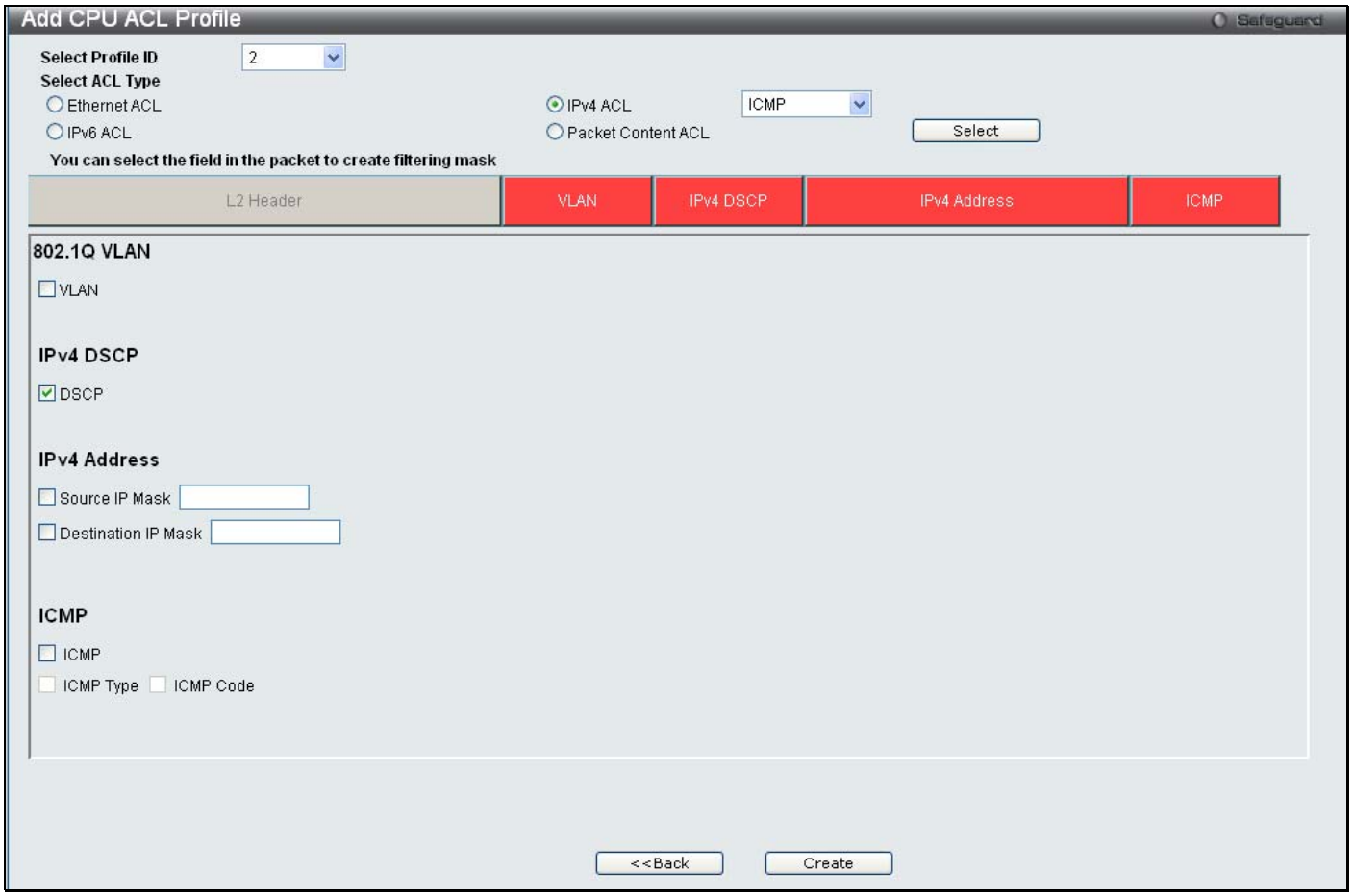


Figure 6 - 36. Add CPU ACL Profile window for IPv4 example

Click on the boxes near the top of the window, which will then turn red and reveal parameters for configuration. To create a new entry, enter the appropriate information and click **Create**. To return to the **CPU Access Profile List** window, click **<<Back**.

The following parameters can be set for IPv4:

Parameter	Description
VLAN	Selecting this option instructs the Switch to examine the VLAN part of each packet header and use this as the, or part of the criterion for forwarding.
IPv4 DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.

IPv4 Address	Tick either Source IP Mask and enter the IPv4 source address mask or Destination IP Mask and enter the IPV4 destination address mask.
ICMP	Tick ICMP to specify that the Switch will examine the Internet Control Message Protocol (ICMP) field within each packet. Tick ICMP Type to specify that the access profile will apply to this ICMP type value. Tick ICMP Code to specify that the access profile will apply to this ICMP code value.
IGMP	Tick IGMP to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header. Tick IGMP Type to further specify that the access profile will apply an IGMP type value.
TCP	Tick TCP to use the TCP port number contained in an incoming packet as the forwarding criterion. Ticking TCP requires specifying a source port mask and/or a destination port mask. The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. T Source Port Mask (0-FFFF) – Tick and specify a TCP port mask for the source port to filter, in hex form (hex 0x0-0xffff). Destination Port Mask (0-FFFF) – Tick and specify a TCP port mask for the destination port to filter, in hex form (hex 0x0-0xffff). TCP Flag Bits – Tick URG (urgent), ACK (acknowledgement), PSH (push), RST (reset), SYN (synchronize), FIN (finish), or Check All to filter certain flag bits within the packets.
UDP	Tick UDP to use the UDP port number contained in an incoming packet as the forwarding criterion. Ticking UDP requires specifying a source port mask and/or a destination port mask. Source Port Mask – Tick and specify a TCP port mask for the source port to filter, in hex form (hex 0x0-0xffff). Destination Port Mask – Tick and specify a TCP port mask for the destination port to filter, in hex form (hex 0x0-0xffff).
Protocol ID	Tick Protocol ID Mask and enter a value defining the protocol ID in the packet header to mask. Protocol ID Mask (0-FF) – Tick and enter a value defining the mask options behind the IP header. User Define (0-FFFFFFFF) – Tick and enter a user-defined value.

Click **Apply** to implement changes made.

Click **Create** to view the new CPU Access Profile List entry in the **CPU Access Profile List** window shown below. To add another Access Profile click **Add CPU ACL Profile**. To delete a profile click the corresponding **Delete** button, to view the specific configurations for an entry click the **Show Details** button. To add a rule to the CPU Access Profile entry, click the **Add/View Rules** button.

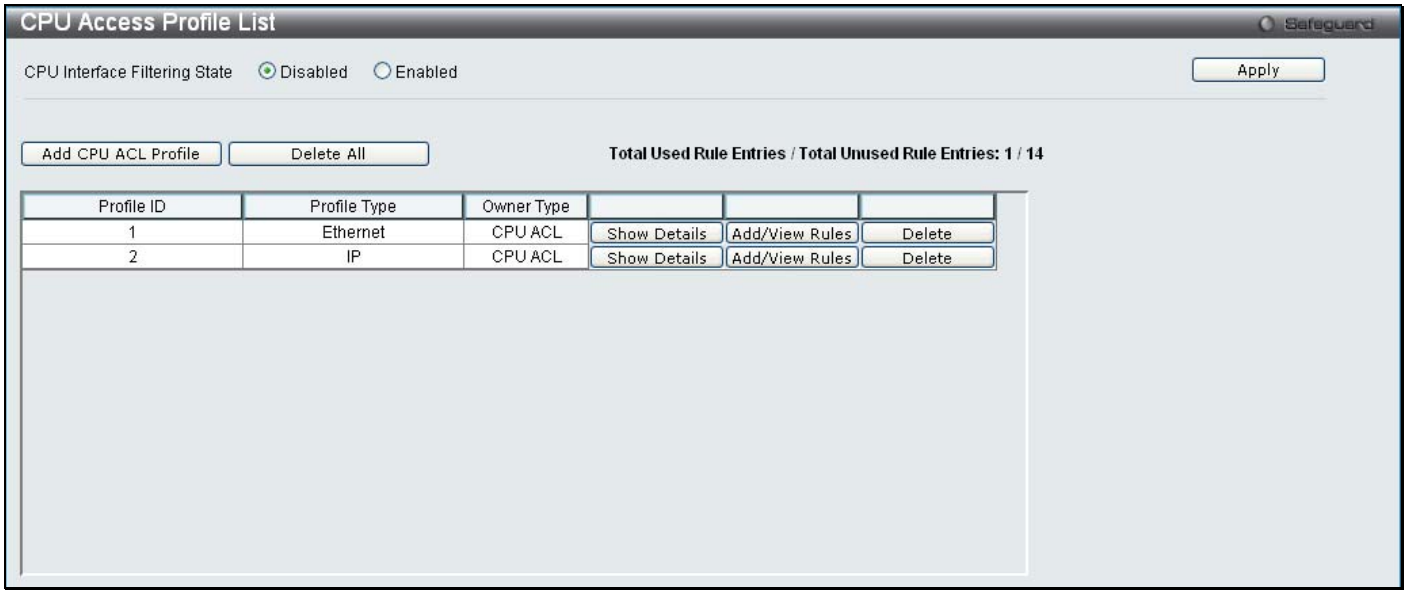


Figure 6 - 37. CPU Access Profile List window for IPv4 example

To view the configurations for a previously configured entry, click on the corresponding **Show Details** button, which will display the following window:

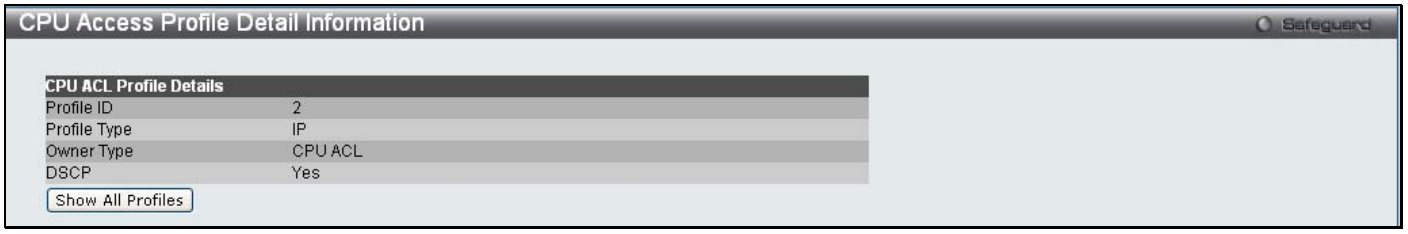


Figure 6 - 38. CPU Access Profile Detail Information window for IPv4 example

To return to the **CPU Access Profile List** window, click **Show All Profiles**. To add a rule to a previously configured entry, click on the corresponding **Add/View Rules** button, and then click **Add Rule** on the **CPU Access Rule List** window, which will reveal the following window:

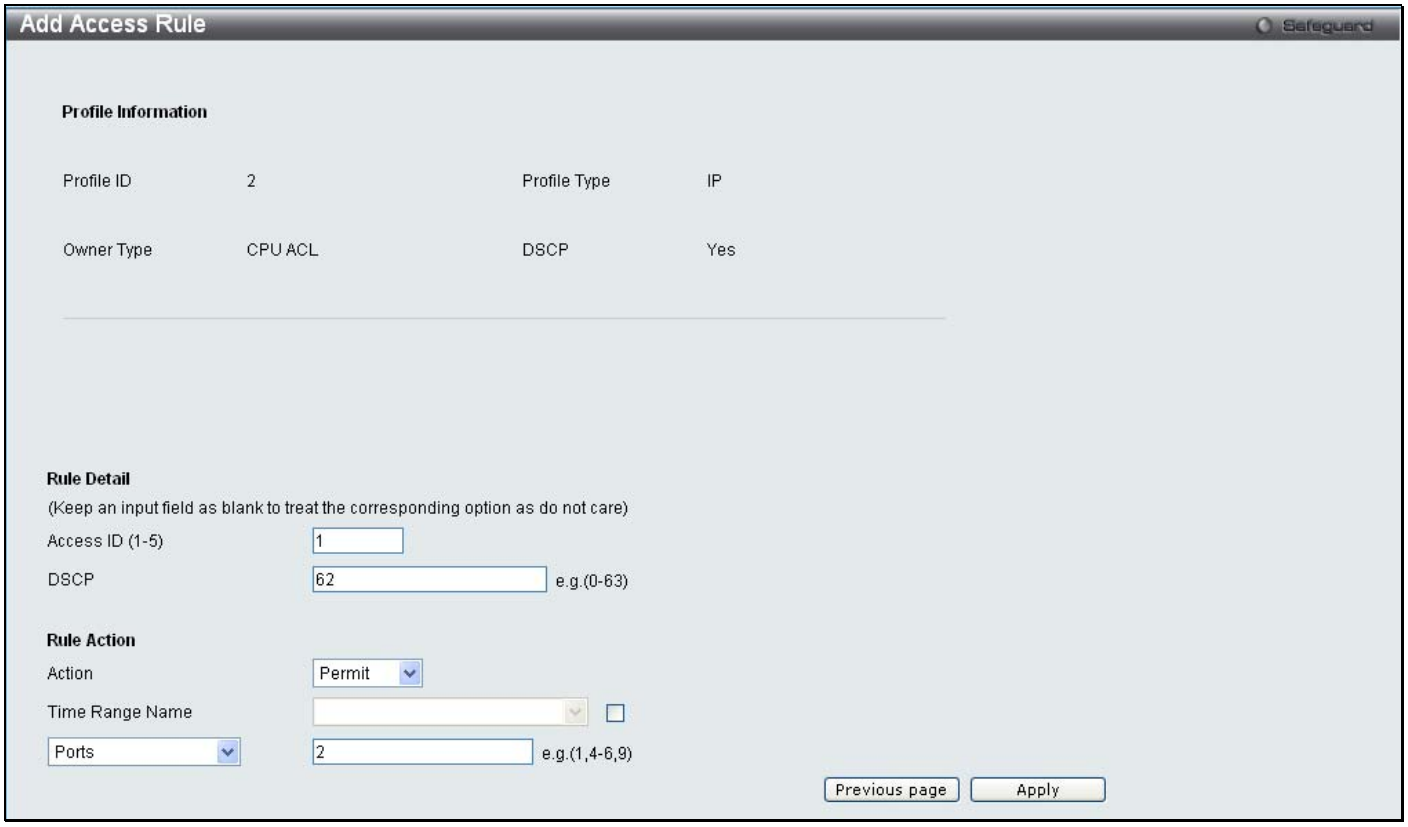


Figure 6 - 39. (CPU) Add Access Rule window for IPv4 example

The following parameters may be configured for the IP (IPv4) filter:

Parameter	Description
Access ID (1-5)	Type in a unique identifier number for this access. This value can be set from *1* to *5*.
DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the criteria, or part of the criterion for forwarding.
ICMP	Select *ICMP* to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify the packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Ports	Enter a range of ports to be configured.

Click **Apply** to display the following **CPU Access Rule List** window:

Figure 6 - 40. CPU Access Rule List window for IPv4 example

To view the configurations for a previously configured rule, click on the corresponding **Show Details** button, which will display the following **CPU Access Rule Detail Information** window:

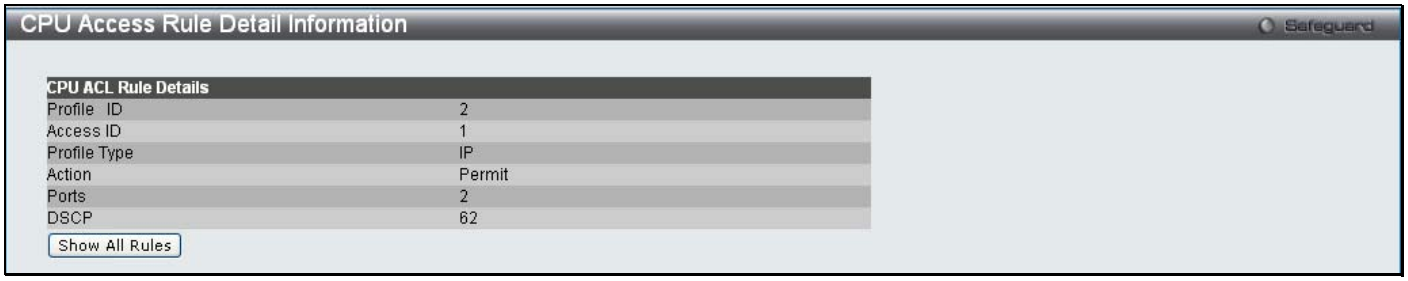


Figure 6 - 41. CPU Access Rule Detail Information window for IPv4 example

To create an IPv6 ACL, click **Add CPU ACL Profile** in the **CPU Access Profile List** window and then use the drop-down menu to select a Profile ID between *1* and *3* and click the IPv6 ACL radio button. Click **Select** and the following window will appear:

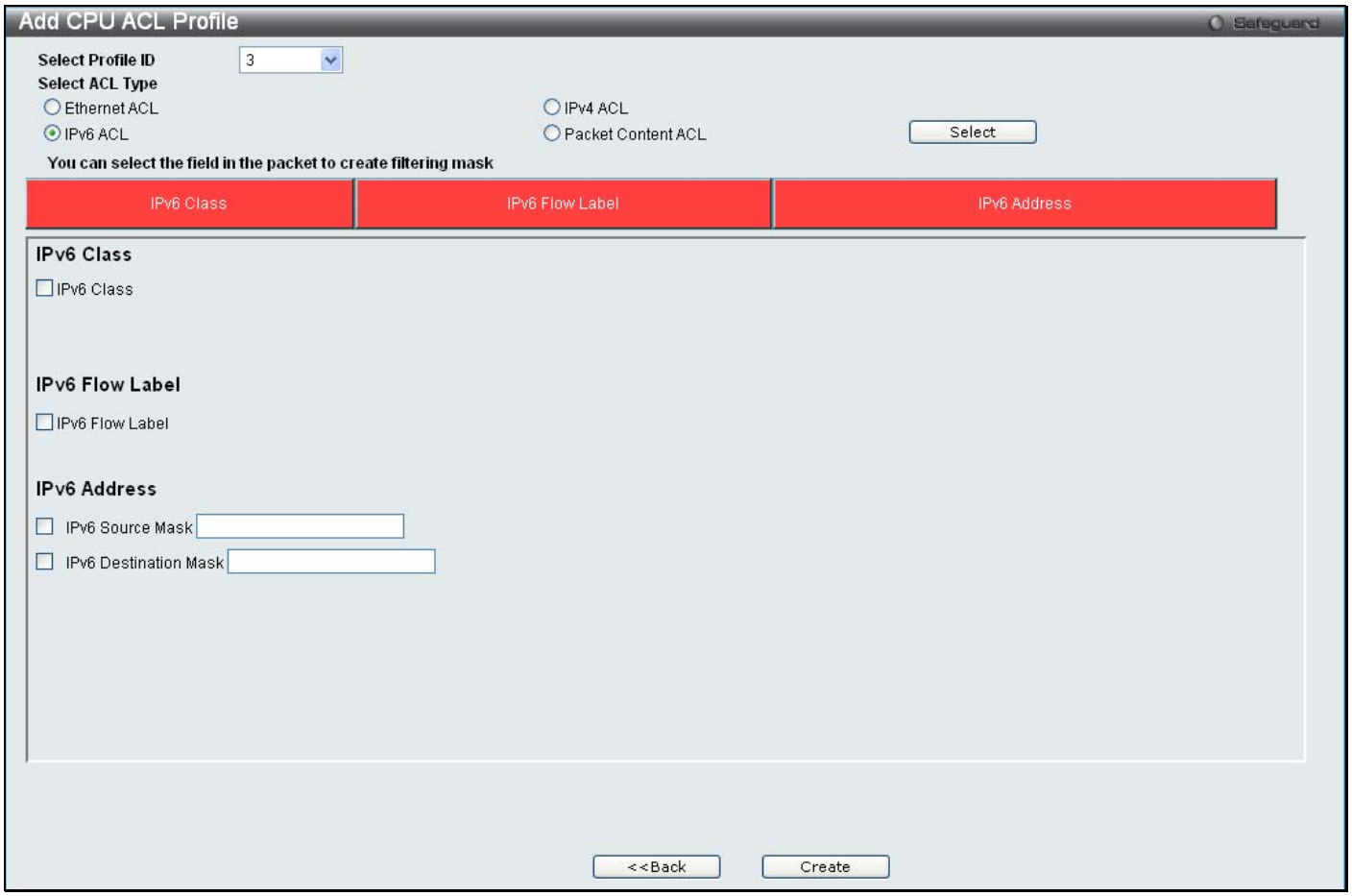


Figure 6 - 42. Add CPU ACL Profile window for IPv6 example

Click on the boxes at the top of the table, which will then turn red and reveal parameters for configuration. To create a new entry enter the correct information and click **Create**. To return to the **CPU Access Profile List** window, click **<<Back**.

The following parameters can be set for IPv6:

Parameter	Description
IPv6 Class	Ticking this check box will instruct the Switch to examine the class field of the IPv6 header. The class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4.
IPv6 Flow Label	Ticking this check box will instruct the Switch to examine the flow label field of the IPv6 header. The flow label field is used by a source to label sequences of packets such as non-

	default quality of service or real time service packets.
IPv6 Address	IPv6 Source Address – Enter an IPv6 address to be used as the source address. IPv6 Destination Address – Enter an IPv6 address that will be used as the destination address. **NOTE:** At any one time the user can only choose IPv6 class and IPv6 Flow Label together or IPv6 Address by itself.

Click **Apply** to implement changes made.

Click **Create** to view the new CPU Access Profile List entry in the **CPU Access Profile List** window shown below. To add another Access Profile, click **Add CPU ACL Profile**. To delete a profile click the corresponding **Delete** button. To view the specific configurations for an entry click, the **Show Details** button. To add a rule to the CPU Access Profile entry, click the **Add/View Rules** button.

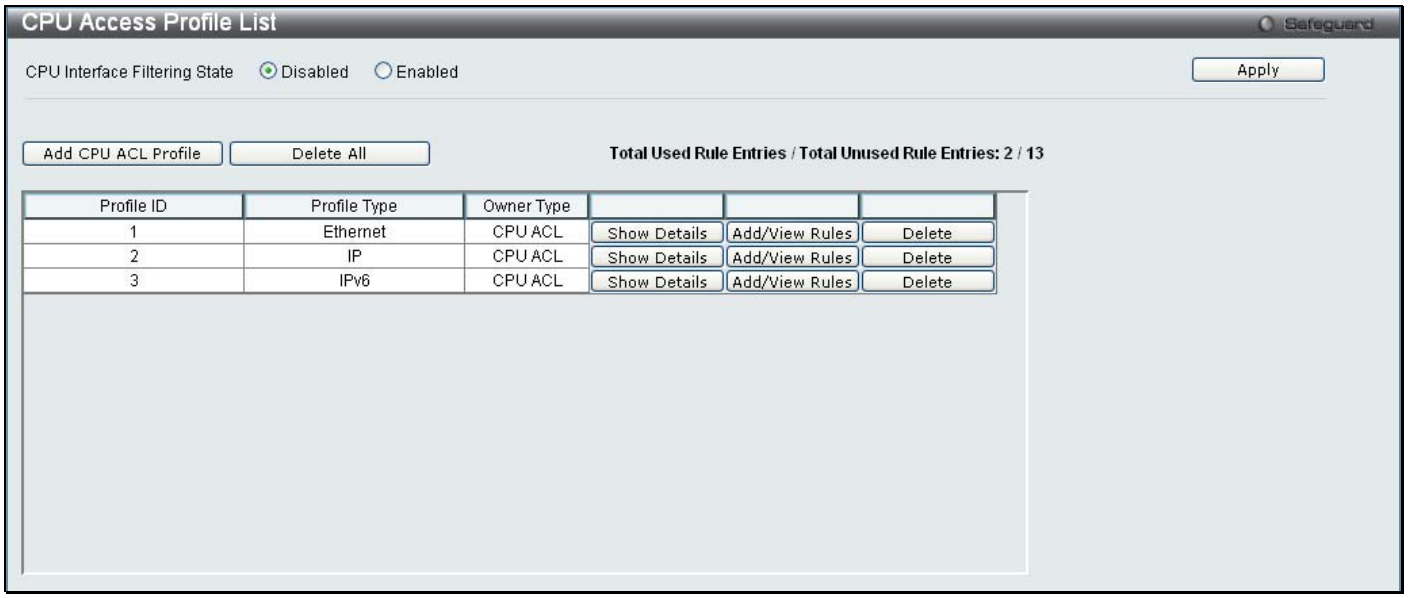


Figure 6 - 43. CPU Access Profile List window for IPv6 example

To view the configurations for a previously configured entry, click on the corresponding **Show Details** button, which will display the following window:

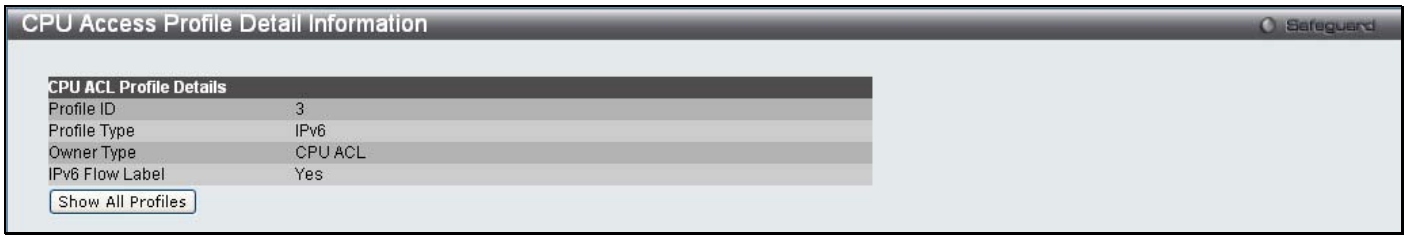


Figure 6 - 44. CPU Access Profile Detail Information window for IPv6 example

To return to the **CPU Access Profile List** window, click **Show All Profiles**. To add a rule to a previously configured entry, click on the corresponding **Add/View Rules** button and then click **Add Rule** on the **CPU Access Rule List** window, which will reveal the following window:

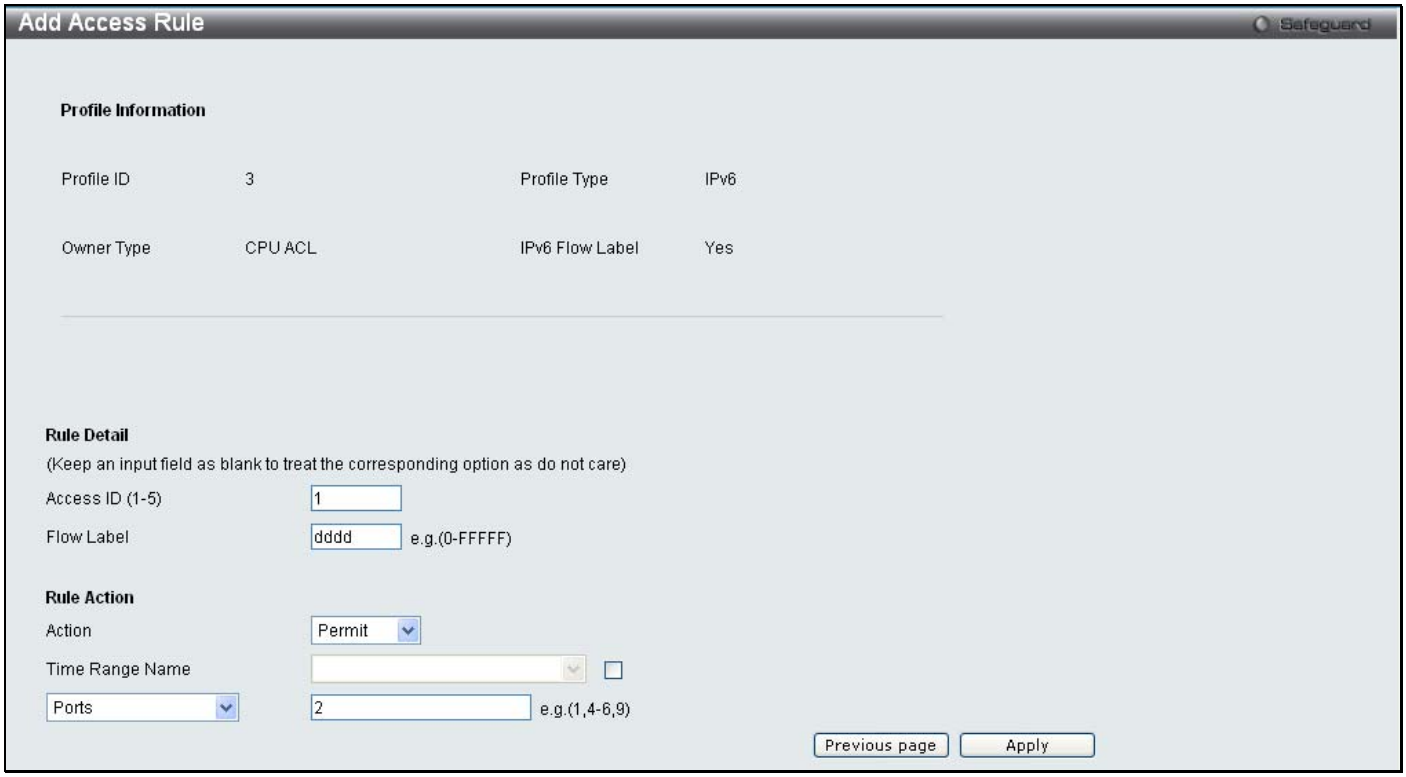


Figure 6 - 45. (CPU) Add Access Rule window for IPv6 example

The following parameters may be configured for the IPv6:

Parameter	Description
Access ID (1-5)	Type in a unique identifier number for this access. This value can be set from *1* to *5*.
Flow Label	Specifies the IPv6 Flow Label. Enter a value between *0 – FFFFF*.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify the packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Ports	Enter a range of ports to be configured.

Click **Apply** to display the following **Access Rule List** window:

Figure 6 - 46. CPU Access Rule List window for IPv6 example

To view the configurations for a previously configured rule, click on the corresponding **Show Details** button, which will display the following **CPU Access Rule Detail Information** window:

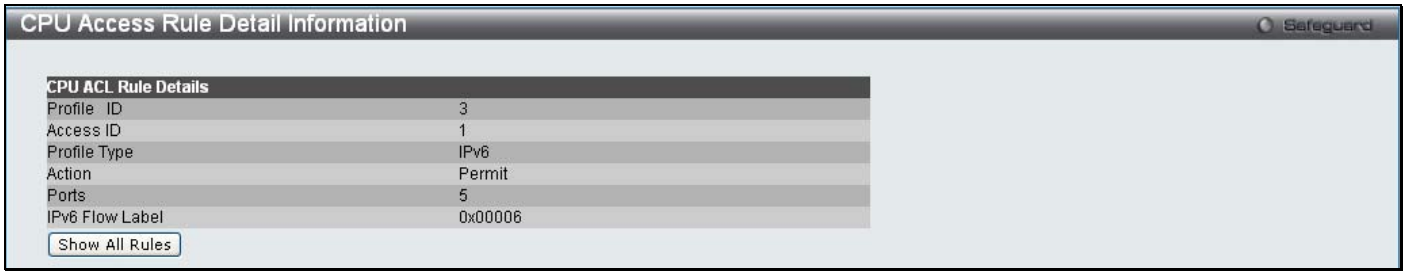


Figure 6 - 47. CPU Access Rule Detail Information window for IPv6 example

To create a Packet Content ACL, click **Add CPU ACL Profile** in the **CPU Access Profile List** window and then use the drop-down menu to select a Profile ID between *1* and *3* and click the Packet Content ACL radio button. Click **Select** and the following window will appear:

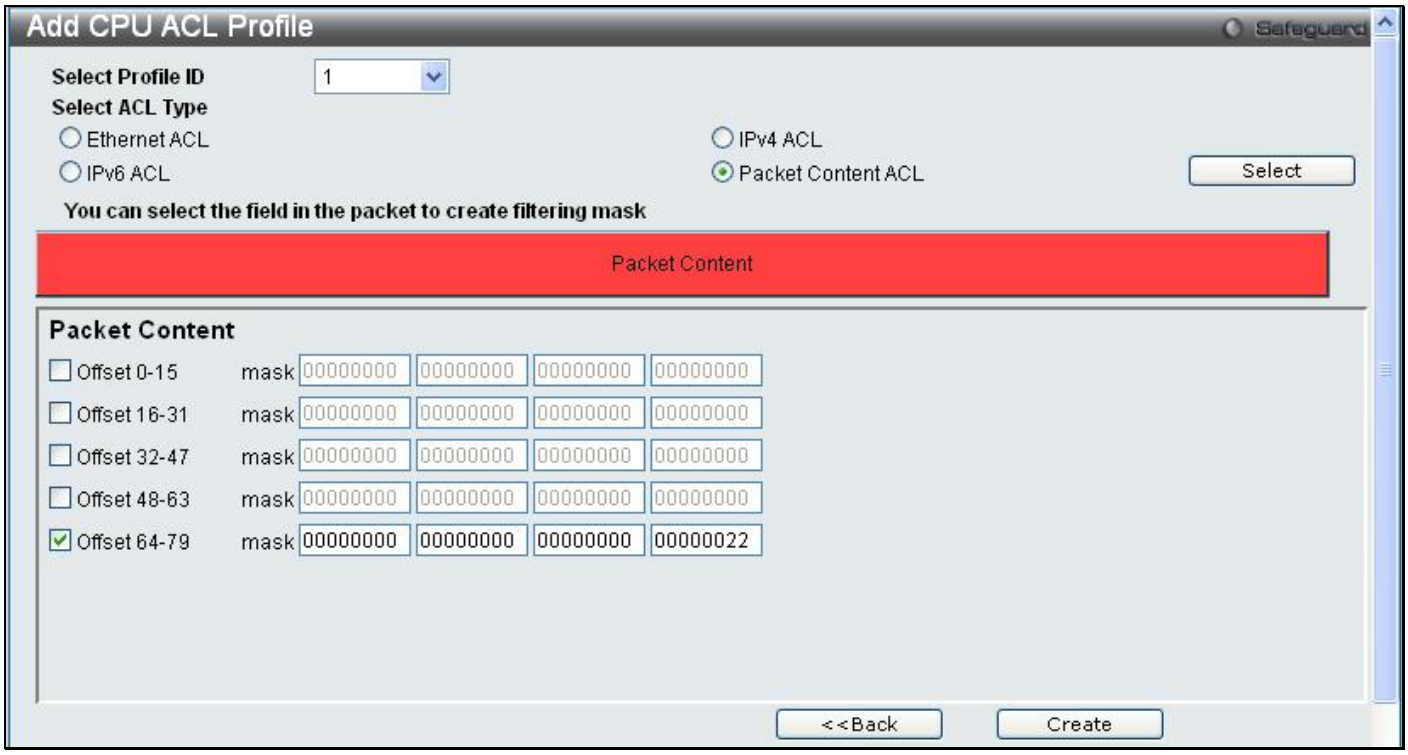


Figure 6 - 48. Add CPU ACL Profile window for Packet Content example

Click on the box at the top of the table, which will then turn red and reveal parameters for configuration. To create a new entry enter the correct information and click **Create**. To return to the **CPU Access Profile List** window, click **<<Back**.

The following parameters can be set for Packet Content:

Parameter	Description
Packet Content	Allows users to examine up to five specified offset packet content chunks within a packet at one time and specifies the frame content offset, mask, and layer. There are five packet content chunk offsets that can be configured. A packet content chunk mask presents four bytes. Up to five packet content offset chunks can be selected: Offset 0-15 mask - Enter a value in hex form to mask the packet from byte 0 to byte 15. Offset 16-31 mask - Enter a value in hex form to mask the packet from byte 16 to byte 31. Offset 32-47 mask - Enter a value in hex form to mask the packet from byte 32 to byte 47. Offset 48-63 mask - Enter a value in hex form to mask the packet from byte 48 to byte 63. Offset 64-79 mask - Enter a value in hex form to mask the packet from byte 64 to byte 79. Note: Only one packet content mask profile can be created. With this advanced unique Packet Content Mask (also known as Packet Content Access Control List - ACL), the D-Link xStack® switch family can effectively mitigate some network attacks like the

	common ARP Spoofing attack that is wide spread today. This is why the Packet Content ACL is able to inspect any specified content of a packet in different protocol layers.

Click **Apply** to implement changes made.

Click **Create** to view the new CPU Access Profile List entry in the **CPU Access Profile List** window shown below. To add another CPU Access Profile, click **Add CPU ACL Profile**. To delete a profile, click the corresponding **Delete** button. To view the specific configurations for an entry, click the **Show Details** button. To add a rule to the CPU Access Profile entry, click the **Add/View Rules** button.

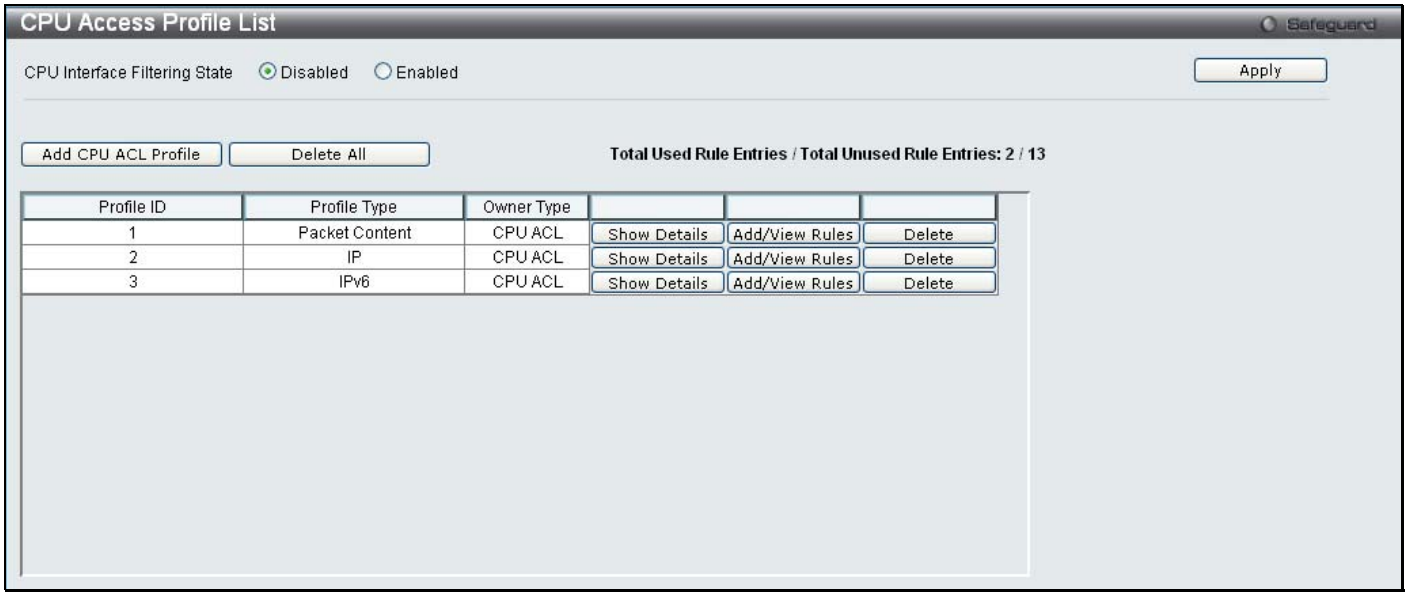


Figure 6 - 49. CPU Access Profile List window for Packet Content example

To view the configurations for a previously configured entry, click on the corresponding **Show Details** button, which will display the following window:

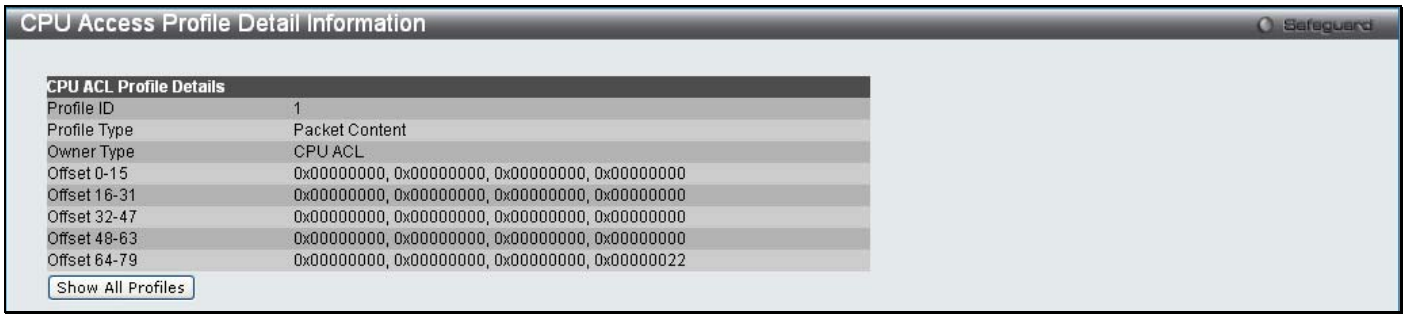


Figure 6 - 50. CPU Access Profile Detail Information window for Packet Content example

To return to the **CPU Access Profile List** window, click **Show All Profiles**. To add a rule to a previously configured entry, click on the corresponding **Add/View Rules** button and then **Add Rule**, which will reveal the following window:

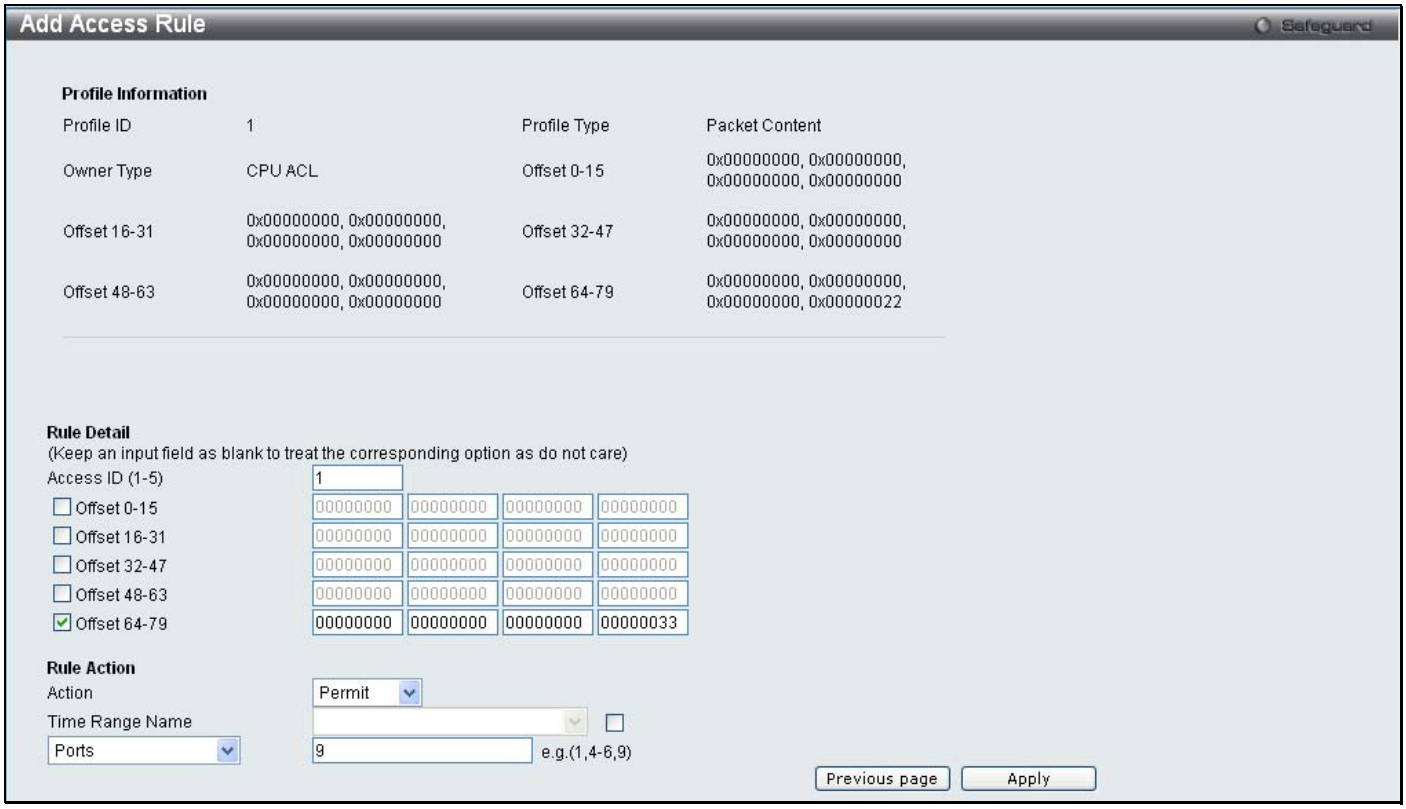

Add Access Rule
Safeguard
Profile Information
Profile ID 1 Profile Type Packet Content
Owner Type CPU ACL Offset 0-15 0x00000000, 0x00000000, 0x00000000, 0x00000000
Offset 16-31 0x00000000, 0x00000000, 0x00000000, 0x00000000 Offset 32-47 0x00000000, 0x00000000, 0x00000000, 0x00000000
Offset 48-63 0x00000000, 0x00000000, 0x00000000, 0x00000000 Offset 64-79 0x00000000, 0x00000000, 0x00000000, 0x00000022
Rule Detail
(Keep an input field as blank to treat the corresponding option as do not care)
Access ID (1-5) 1
Offset 0-15
Offset 16-31
Offset 32-47
Offset 48-63
Offset 64-79 00000000 00000000 00000000 00000033
Rule Action
Action Permit
Time Range Name
Ports 9 e.g.(1,4-6,9)
Previous page
Apply

Figure 6 - 51. (CPU) Add Access Rule window for Packet Content example

The following parameters may be configured for the Packet Content filter:

Parameter	Description
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify the packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Rule Detail	This field will instruct the Switch to mask the packet header beginning with the offset value specified: Offset 0-15 – Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte. Offset 16-31 – Enter a value in hex form to mask the packet from byte 16 to byte *31.* Offset 32-47 – Enter a value in hex form to mask the packet from byte 32 to byte 47. Offset 48-63 – Enter a value in hex form to mask the packet from byte 48 to byte 63. Offset 64-79 – Enter a value in hex form to mask the packet from byte 64 to byte 79.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Ports	Enter a range of ports to be configured.

Click **Apply** to display the following **CPU Access Rule List** window:

Figure 6 - 52. CPU Access Rule List window for Packet Content example

To view the configurations for previously configured rule click on the corresponding **Show Details** Button which will display the following **CPU Access Rule Detail Information** window.

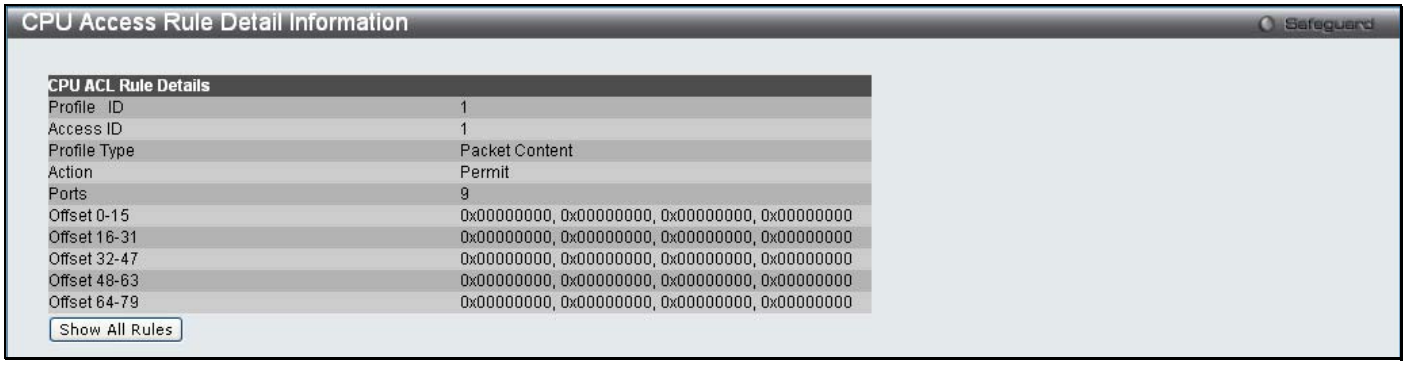


Figure 6 - 53. CPU Access Rule Detail Information window for Packet Content example

ACL Finder

This window is used to help find a previously configured ACL entry. To search for an entry, select the profile ID from the drop-down menu, enter a port to view, define the state (*Normal* or *CPU*) and click **Find,** the table on the lower half of the window will display the entries. To delete an entry click the corresponding **Delete** button.

To open this window, click **ACL > ACL Finder**

Figure 6 - 54. ACL Finder window

ACL Flow Meter

This window offers flow bandwidth control used to limit the bandwidth of the ingress traffic. When users create an ACL rule to filter packets, a metering rule can be created to associate with this ACL rule to limit traffic. The step of bandwidth is 64kbps. Due to limited metering rules, not all ACL rules can associate with a metering rule.

To open this window, click **ACL > ACL Flow Meter**

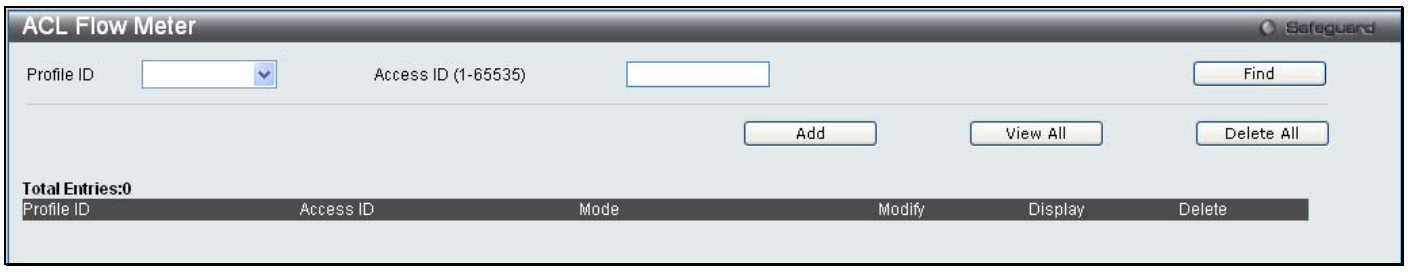


Figure 6 - 55. ACL Flow Meter window

The following fields may be configured:

Parameter	Description
Profile ID	The pre-configured Profile ID for which to configure the Flow Metering parameters.
Access ID (1-65535)	The pre-configured Access ID for which to configure the Flow Metering parameters.

Enter the appropriate information and click **Find**. The entries will be displayed on the lower half of the table. To edit an entry, click the corresponding **Modify** button. To delete an entry, click the corresponding **Delete** button. To add a new entry, click the **Add** button, which will display the following window for the user to configure:

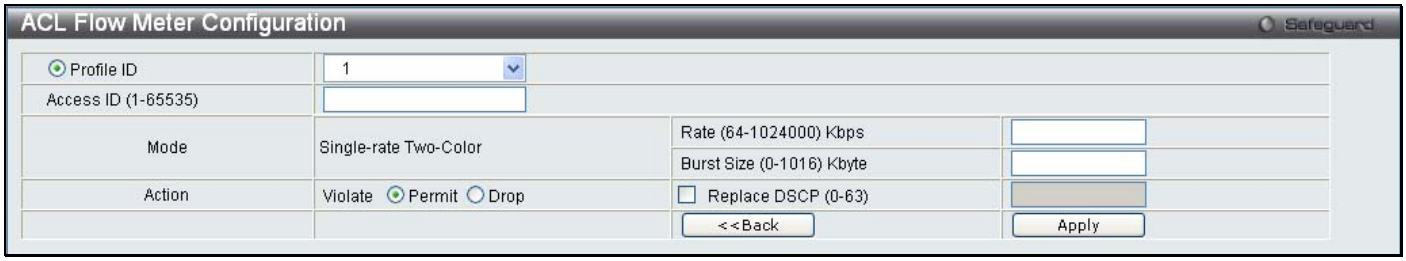


Figure 6 - 56. ACL Flow Meter Configuration window

The following fields may be configured:

Parameter	Description
Profile ID	Use the drop-down menu to select the pre-configured Profile ID that will be used to configure the Flow Metering parameters.
Access ID (1-65535)	Enter the Access ID that will be used to configure the Flow Metering parameters, enter a value between *1* and *65535*.
Mode	Single-rate Two-Color Marker, marks packets green or red based on a rate and burst size. This is useful when only burst size matters. • Rate (64-1024000) Kbps – Specifies the committed bandwidth in Kbps for the flow. The range is from *64* to *1024000*. The unit is Kbps. • Burst Size (0-1016) Kbyte – Specifies the burst size for this flow. The range is from *0* to *1016*. The unit is Kbyte.
Action	Violate – Specifies the action when the packet is in “red color” mode. • Permit – Permits the packet. • Replace DSCP – Change the DSCP of the packet. • Drop – Drops the packet.

Click **Apply** to implement changes made, click **<<Back** to return to the **ACL Flow Meter** window.

Section 7

Monitoring

Cable Diagnostic
CPU Utilization
Port Utilization
Packet Size
Memory Utilization
Packets
Errors
Port Access Control
Browse ARP Table
Browse VLAN
IGMP Snooping
LLDP
MBA Authentication State
Browse Session Table
MAC Address Table
System Log

Cable Diagnostic

This window displays the details of copper cables attached to specific ports on the Switch. If there is an error in the cable this feature can determine the type of error and the position where the error has occurred.

To view this window, click **Monitoring > Cable Diagnostic**:

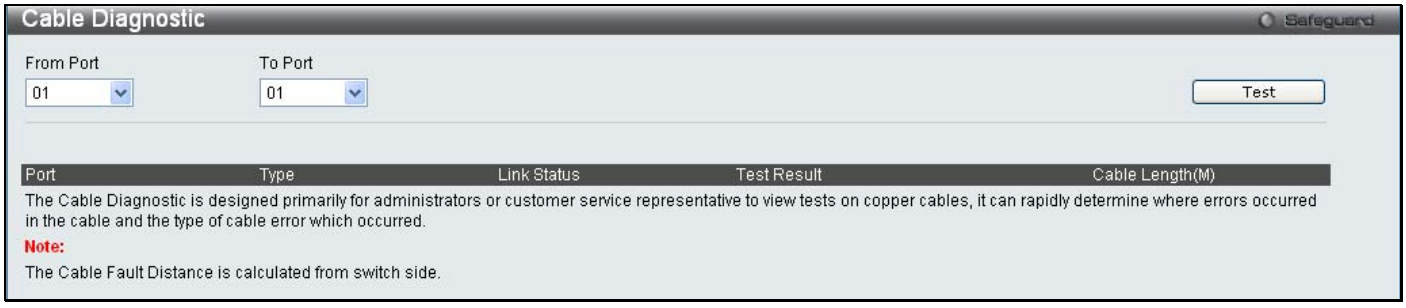

Cable Diagnostic
Safeguard
From Port
01
To Port
01
Test
Port
Type
Link Status
Test Result
Cable Length(M)
The Cable Diagnostic is designed primarily for administrators or customer service representative to view tests on copper cables, it can rapidly determine where errors occurred in the cable and the type of cable error which occurred.
Note:
The Cable Fault Distance is calculated from switch side.

Figure 7 - 1. Cable Diagnostic window

Enter the range of ports to test and click **Test**. The results will be displayed in the table on the lower half of the window.

CPU Utilization

This window displays the percentage of the CPU being used, expressed as an integer percentage and calculated as a simple average by time interval.

To view this window, click **Monitoring > CPU Utilization**:

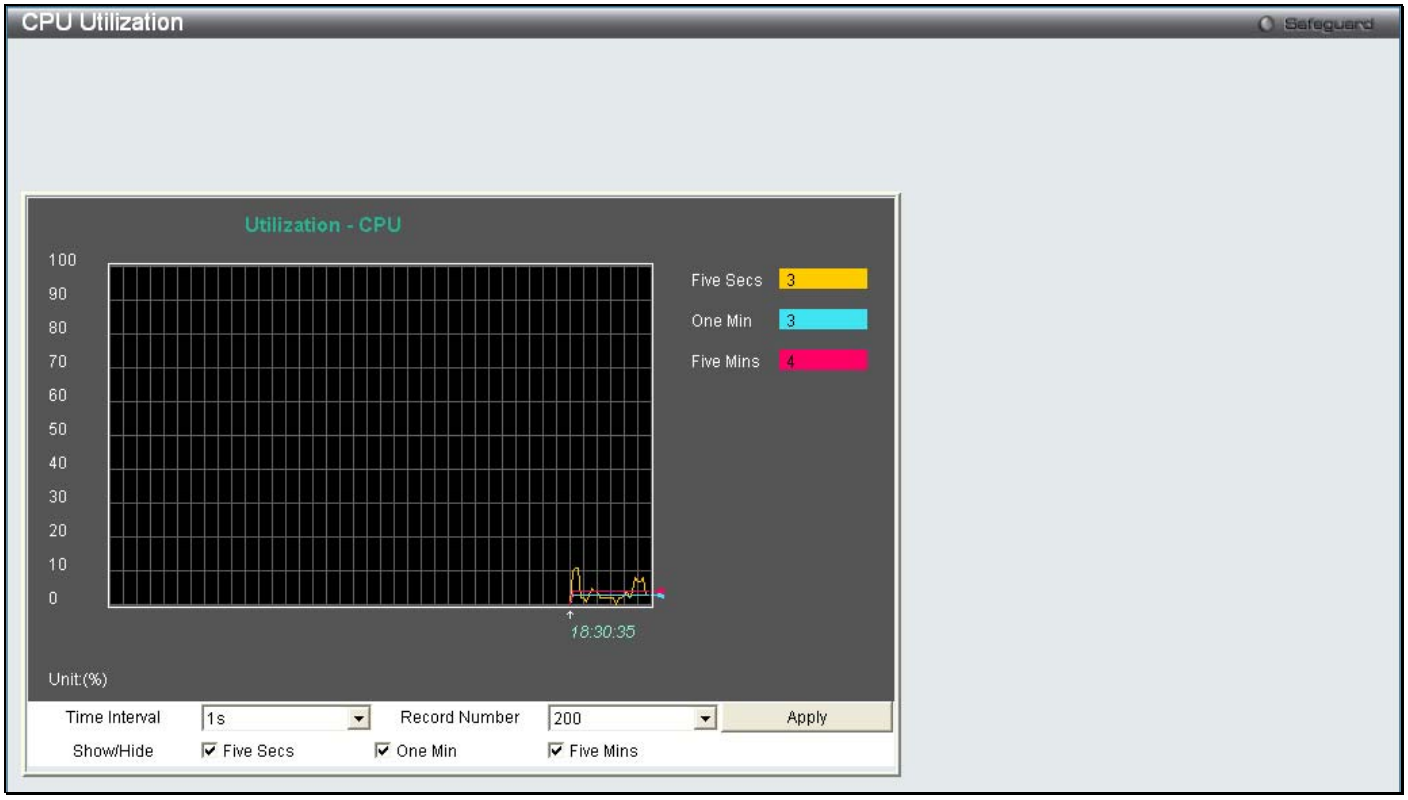


Figure 7 - 2. CPU Utilization window

To view the CPU utilization by port, use the real-time graphic of the Switch at the top of the Web page by simply clicking on a port. Click **Apply** to implement the configured settings. The window will automatically refresh with new updated statistics.

Change the view parameters as follows:

Parameter	Description
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Show/Hide	Check whether or not to display Five Secs, One Min, and Five Mins.

Port Utilization

This window displays the percentage of the total available bandwidth being used on the port.

To view this window, click **Monitoring > Port Utilization**:

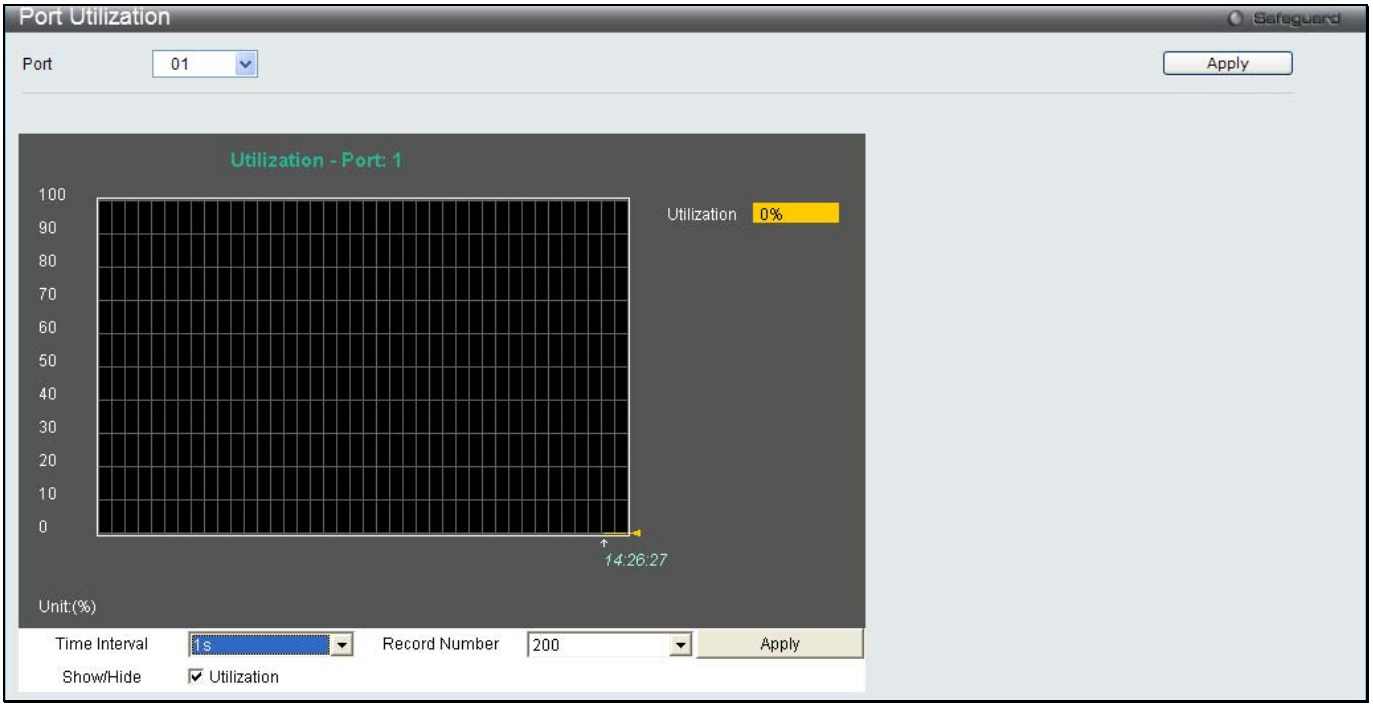


Figure 7 - 3. Port Utilization window

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the Web page by simply clicking on a port.

Change the view parameters as follows:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Show/Hide	Check whether or not to display Utilization.

Packet Size

The Web Manager allows packets received by the Switch, arranged in six groups and classed by size, to be viewed as either a line graph or a table. Two windows are offered. To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the Web page by simply clicking on a port.

To view the packet size windows, click **Monitoring > Packet Size**:

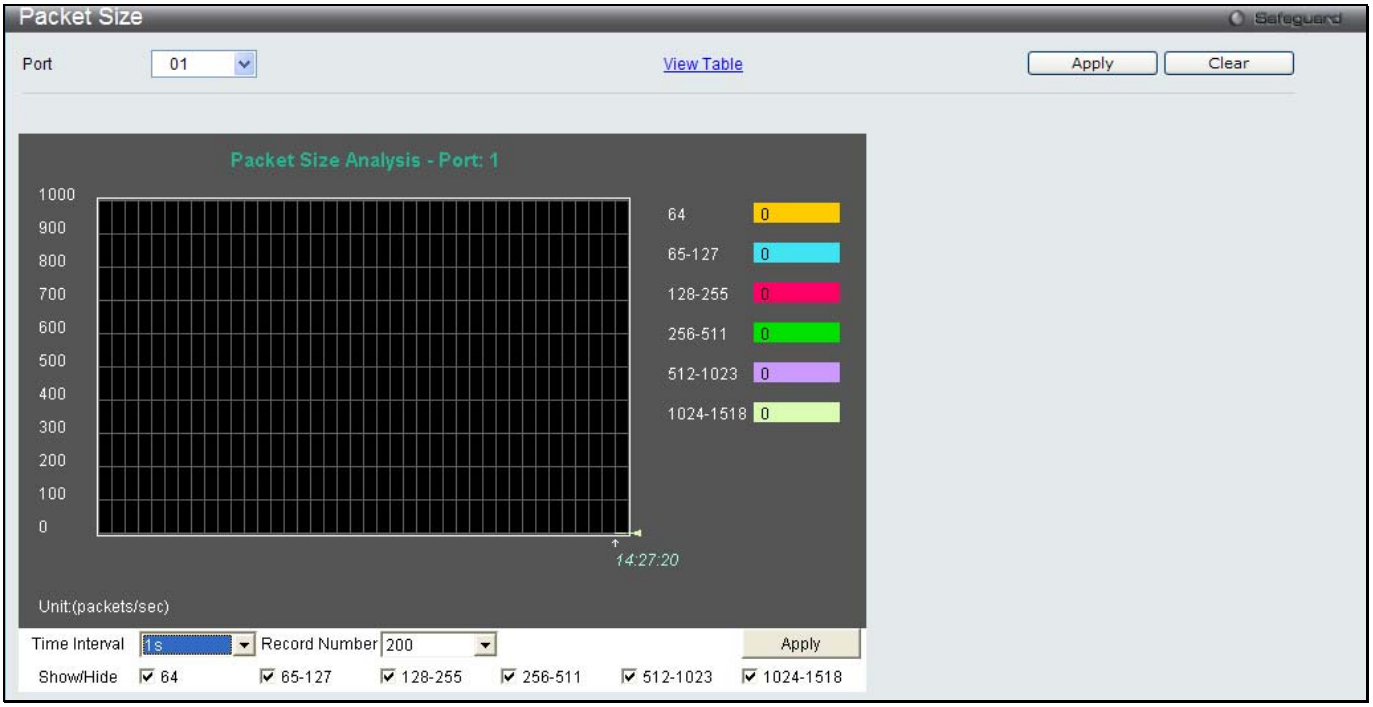


Figure 7 - 4. Packet Size window

To view the **Packet Size Table** window, click the link View Table, which will show the following table:

Figure 7 - 5. Packet Size Table window

The following fields can be set or viewed:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is 200.
64	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

65-127	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256-511	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Show/Hide	Check whether or not to display 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 packets received.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the Switch to display a line graph rather than a table.

Memory Utilization

The Switch displays memory utilization information for DRAM and Flash.

To view this window, click **Monitoring > Memory Utilization**:

Figure 7 - 6. Memory Utilization window

Packets

The Web Manager allows various packet statistics to be viewed as either a line graph or a table. Six windows are offered.

Received (Rx)

These windows display the Rx packets on the Switch. To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the Web page by simply clicking on a port.

To view the following graph of packets received on the Switch, click **Monitoring > Packets > Received (Rx)**:

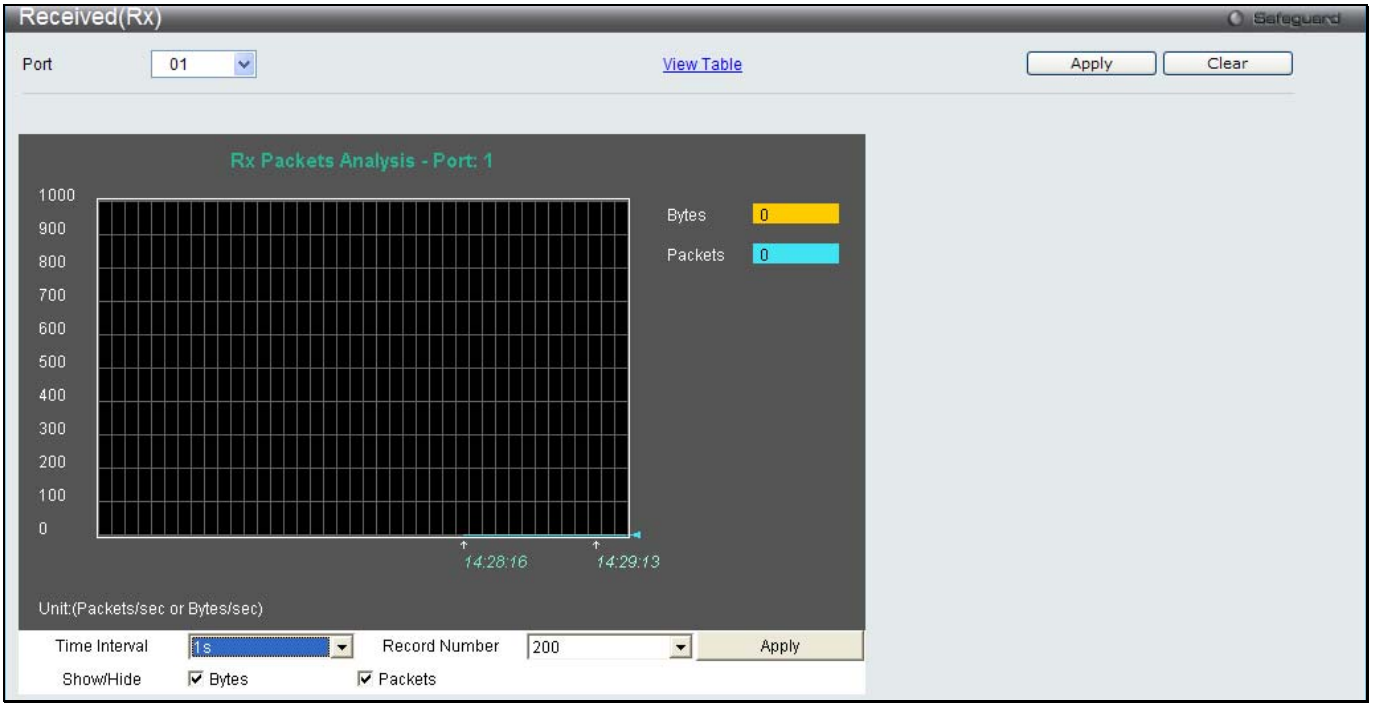


Figure 7 - 7. Received (Rx) window (for Bytes and Packets)

To view the **Received (Rx) Table** window, click View Table.

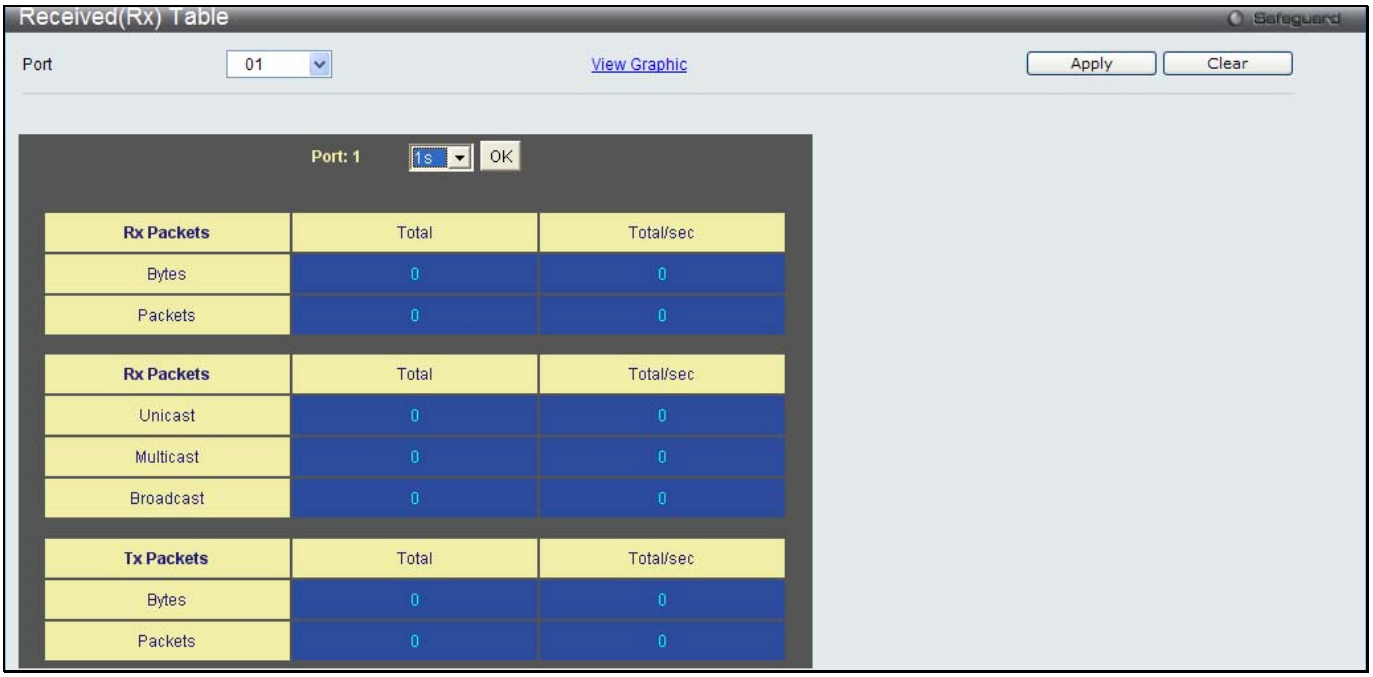


Figure 7 - 8. Received (Rx) Table window (for Bytes and Packets)

The following fields may be set or viewed:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "*s*" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Bytes	Counts the number of bytes received on the port.

Packets	Counts the number of packets received on the port.
Unicast	Counts the total number of good packets that were received by a unicast address.
Multicast	Counts the total number of good packets that were received by a multicast address.
Broadcast	Counts the total number of good packets that were received by a broadcast address.
Show/Hide	Check whether to display Bytes and Packets.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the Switch to display a line graph rather than a table.

UMB_cast (Rx)

These windows display the UMB_cast Rx packets on the Switch. To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the Web page by simply clicking on a port.

To view the following graph of UMB cast packets received on the Switch, click **Monitoring > Packets > UMB_cast (Rx)**:

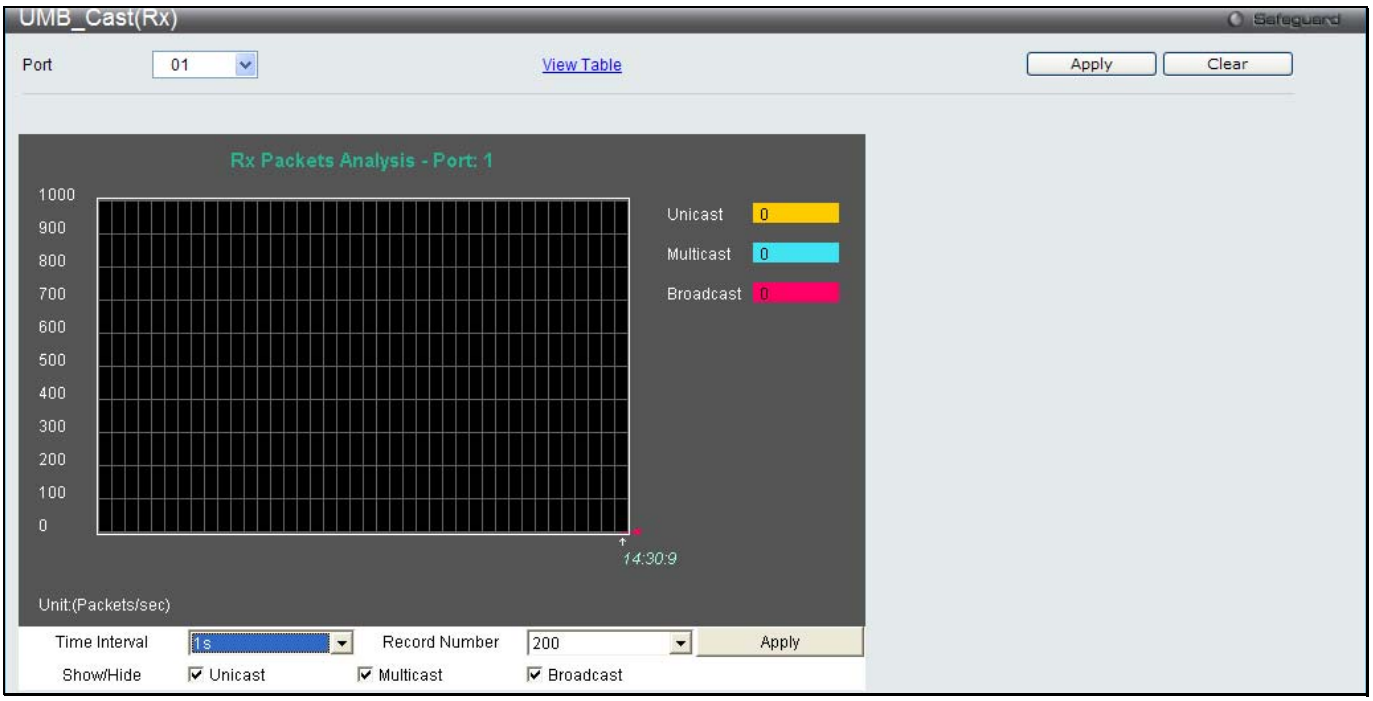


Figure 7 - 9. UMB_cast (Rx) window (for Unicast, Multicast, and Broadcast Packets)

To view the **UMB_cast (Rx) Table** window, click the View Table link.

Figure 7 - 10. UMB_cast (Rx) Table window (for Unicast, Multicast, and Broadcast Packets)

The following fields may be set or viewed:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "*s*" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Unicast	Counts the total number of good packets that were received by a unicast address.
Multicast	Counts the total number of good packets that were received by a multicast address.
Broadcast	Counts the total number of good packets that were received by a broadcast address.
Show/Hide	Check whether or not to display Multicast, Broadcast, and Unicast Packets.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the Switch to display a line graph rather than a table.

Transmitted (Tx)

These windows display the Transmittd (Tx) packets on the Switch.To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the Web page by simply clicking on a port.

To view the following graph of packets transmitted from the Switch, click **Monitoring > Packets > Transmitted (Tx)**:

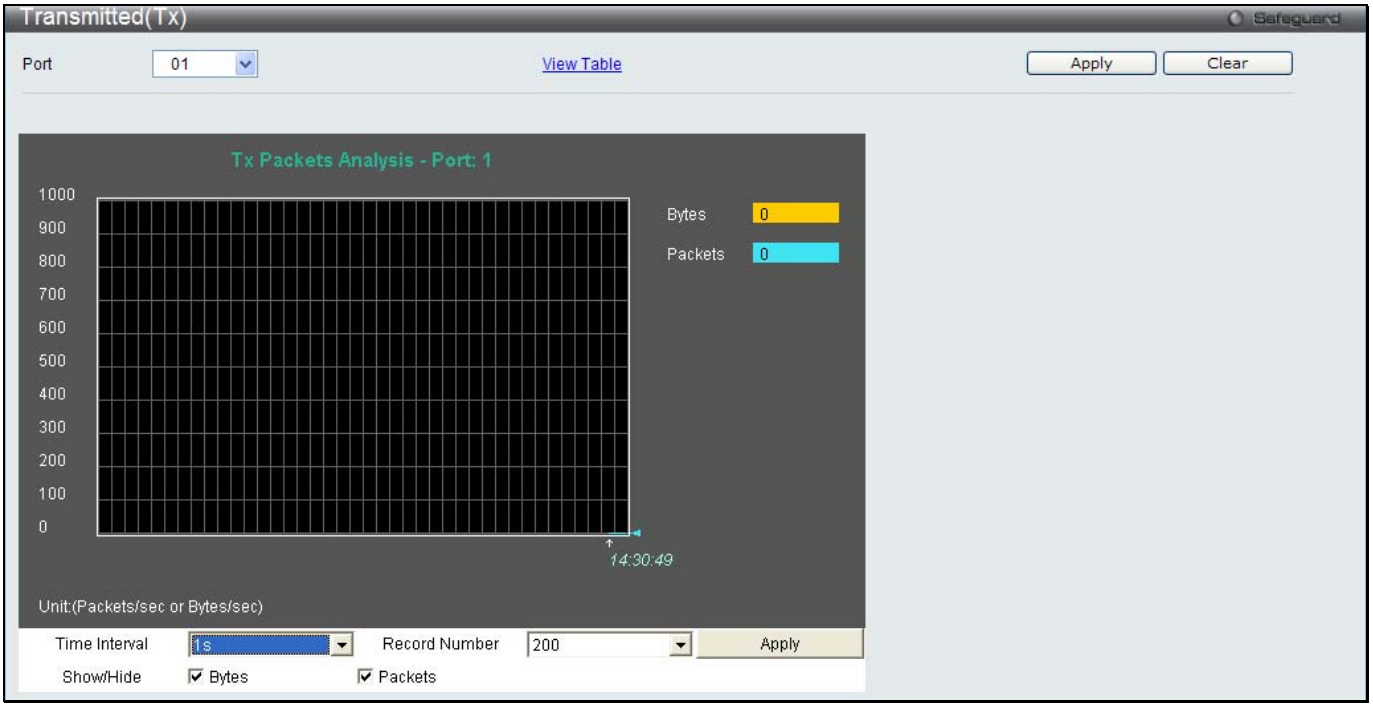


Figure 7 - 11. Transmitted (Tx) window (for Bytes and Packets)

To view the **Transmitted (Tx) Table** window, click the link View Table.

Figure 7 - 12. Transmitted (Tx) Table window (for Bytes and Packets)

The following fields may be set or viewed:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "*s*" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Bytes	Counts the number of bytes successfully sent on the port.

Packets	Counts the number of packets successfully sent on the port.
Unicast	Counts the total number of good packets that were transmitted by a unicast address.
Multicast	Counts the total number of good packets that were transmitted by a multicast address.
Broadcast	Counts the total number of good packets that were transmitted by a broadcast address.
Show/Hide	Check whether or not to display Bytes and Packets.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the Switch to display a line graph rather than a table.

Errors

The Web Manager allows port error statistics compiled by the Switch's management agent to be viewed as either a line graph or a table. Four windows are offered.

Received (RX)

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the Web page by simply clicking on a port.

To view the following graph of error packets received on the Switch, click **Monitoring > Errors > Received (RX)**:

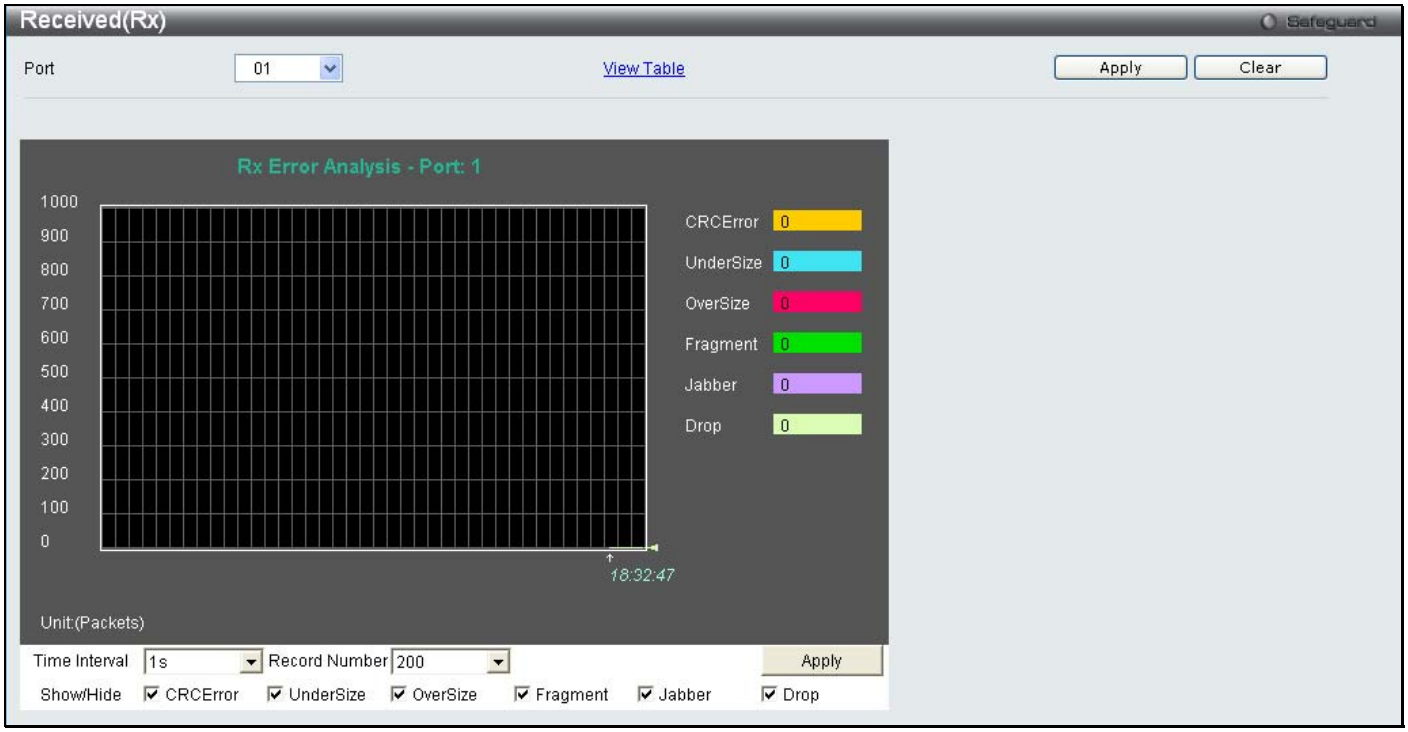


Figure 7 - 13. Received (Rx) window (for errors)

To view the **Received (Rx) Table** window for errors, click the link View Table, which will show the following table:

Figure 7 - 14. Received (Rx) Table window (for errors)

The following fields can be set:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "*s*" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
CRCError	Counts otherwise valid packets that did not end on a byte (octet) boundary.
UnderSize	The number of packets detected that are less than the minimum permitted packets size of 64 bytes and have a good CRC. Undersize packets usually indicate collision fragments, a normal network occurrence.
OverSize	Counts valid packets received that were longer than 1518 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1536.
Fragment	The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
Jabber	Counts invalid packets received that were longer than 1518 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1536.
Drop	The number of packets that are dropped by this port since the last Switch reboot.
Show/Hide	Check whether or not to display CRCError, UnderSize, OverSize, Fragment, Jabber, Drop, and SymbolErr errors.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the Switch to display a line graph rather than a table.

Transmitted (TX)

To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the Web page by simply clicking on a port.

To view the following graph of error packets received on the Switch, click the **Monitoring > Errors > Transmitted (Tx)** :

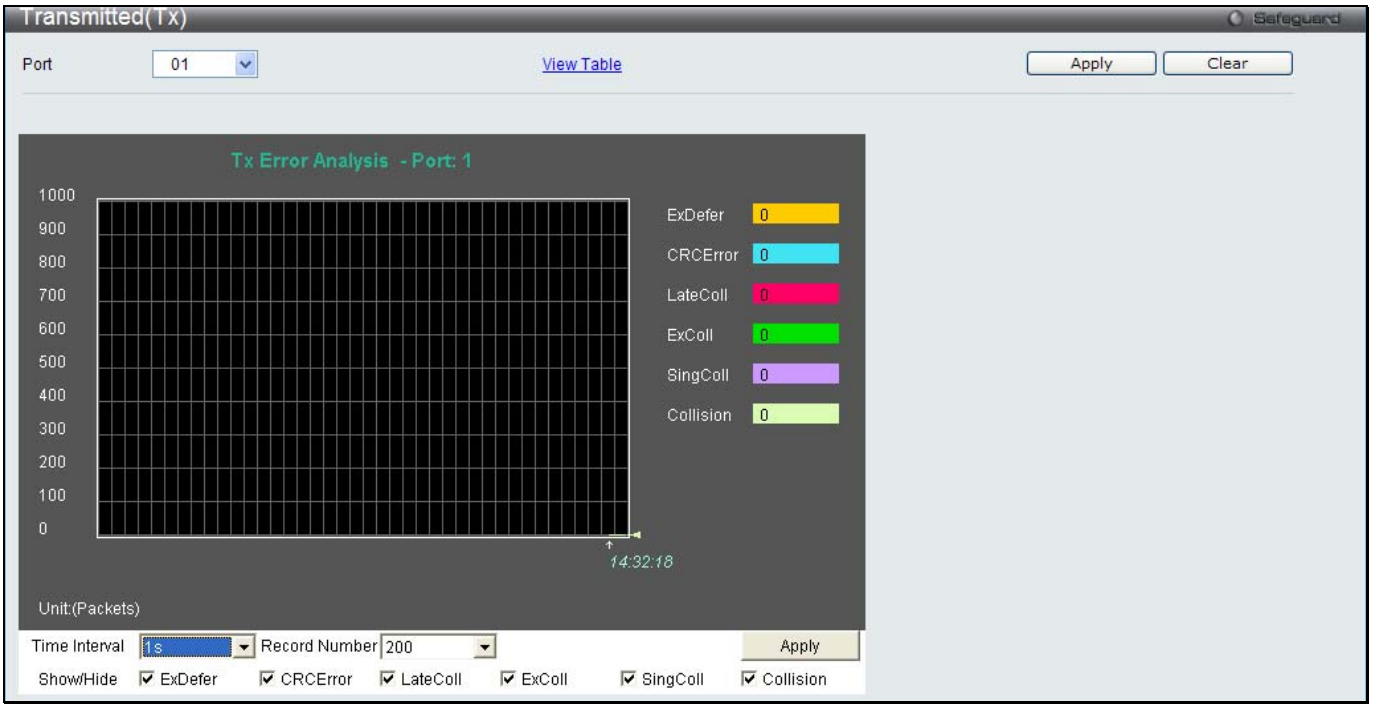


Figure 7 - 15. Transmitted (Tx) window (for errors)

To view the **Transmitted (Tx) Table** window, click the link View Table, which will show the following table:

Figure 7 - 16. Transmitted (Tx) Table window (for errors)

The following fields may be set or viewed:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.

Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
ExDefer	Counts the number of packets for which the first transmission attempt on a particular interface was delayed because the medium was busy.
CRC Error	Counts otherwise valid packets that did not end on a byte (octet) boundary.
LateColl	Counts the number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
ExColl	Excessive Collisions. The number of packets for which transmission failed due to excessive collisions.
SingColl	Single Collision Frames. The number of successfully transmitted packets for which transmission is inhibited by more than one collision.
Collision	An estimate of the total number of collisions on this network segment.
Show/Hide	Check whether or not to display ExDefer, CRCError, LateColl, ExColl, SingColl, and Collision errors.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Graphic	Clicking this button instructs the Switch to display a line graph rather than a table.

Port Access Control

The following six windows are used to monitor 802.1X statistics of the Switch, on a per port basis.

RADIUS Authentication

This table contains information concerning the activity of the RADIUS authentication client on the client side of the RADIUS authentication protocol.

To view the **RADIUS Authentication** window, click **Monitoring > Port Access Control > RADIUS Authentication**:

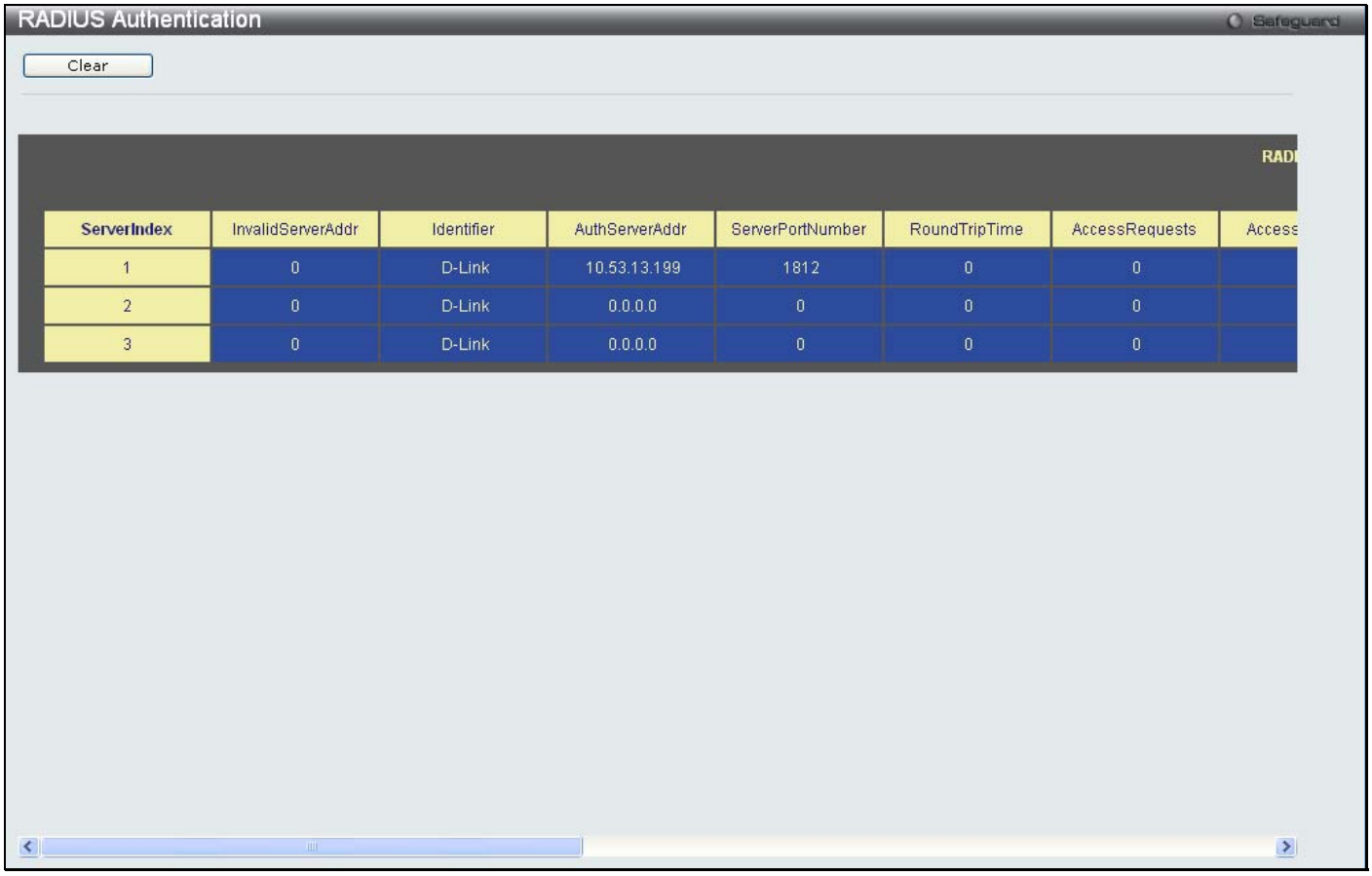


Figure 7 - 17. RADIUS Authentication window

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second. To clear the current statistics shown, click the *Clear* button in the top left hand corner.

The following information is displayed:

Parameter	Description
InvalidServerAddresses	The number of RADIUS Access-Response packets received from unknown addresses.
Identifier	The NAS-Identifier of the RADIUS authentication client. (This is not necessarily the same as sysName in MIB II.)
ServerIndex	The identification number assigned to each RADIUS Authentication server that the client shares a secret with.
AuthServerAddress	The (conceptual) table listing the RADIUS authentication servers with which the client shares a secret.
ServerPortNumber	The UDP port the client is using to send requests to this server.
RoundTripTime	The time interval (in hundredths of a second) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
AccessRequests	The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.
AccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to this RADIUS

	authentication server.
AccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
AccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
AccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
AccessResponses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or known types are not included as malformed access responses.
BadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server.
PendingRequests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject or Access-Challenge, a timeout or retransmission.
Timeouts	The number of authentication timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
UnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the authentication port
PacketsDropped	The number of RADIUS packets of which were received from this server on the authentication port and dropped for some other reason.

RADIUS Account Client

This window shows managed objects used for managing RADIUS accounting clients, and the current statistics associated with them.

To view the **RADIUS Account Client** window, click **Monitoring > Port Access Control > RADIUS Account Client**:

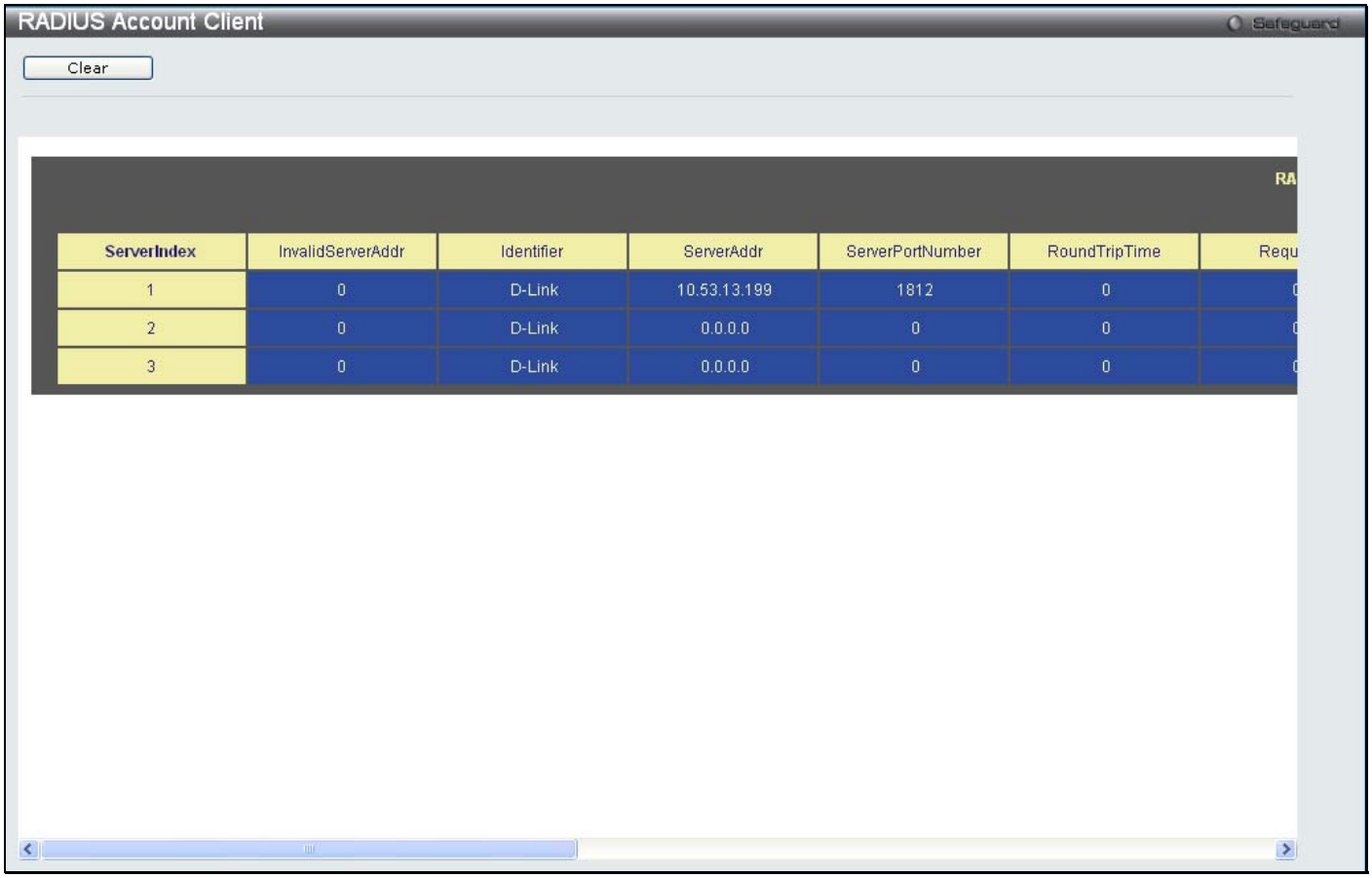


Figure 7 - 18. RADIUS Account Client window

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second. To clear the current statistics shown, click the *Clear* button in the top left hand corner.

The following information is displayed:

Parameter	Description
InvalidServerAddresses	The number of RADIUS Accounting-Response packets received from unknown addresses.
Identifier	The NAS-Identifier of the RADIUS account. (This is not necessarily the same as sysName in MIB II.)
ServerIndex	The identification number assigned to each RADIUS Accounting server that it shares a secret with.
ServerAddress	The (conceptual) table listing the RADIUS accounting servers with which it shares a secret.
ServerPortNumber	The UDP port it is using to send requests to this server.
RoundTripTime	The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.
Responses	The number of RADIUS packets received on the accounting port from this server.
MalformedResponses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting

	responses.
BadAuthenticators	The number of RADIUS Accounting-Response packets, which contained invalid authenticators, received from this server.
PendingRequests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.
Timeouts	The number of accounting timeouts to this server. After a timeout it may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
UnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
PacketsDropped	The number of RADIUS packets, which were received from this server on the accounting port and dropped for some other reason.

Authenticator State

The following section describes the 802.1X State on the Switch.

To view the Authenticator State, click **Monitoring > Port Access Control > Authenticator State**:

Port	Auth_PAE_State	Backend_State	PortStatus
1	ForceAuth	Success	Authorized
2	ForceAuth	Success	Authorized
3	ForceAuth	Success	Authorized
4	ForceAuth	Success	Authorized
5	ForceAuth	Success	Authorized
6	ForceAuth	Success	Authorized
7	ForceAuth	Success	Authorized
8	ForceAuth	Success	Authorized
9	ForceAuth	Success	Authorized
10	ForceAuth	Success	Authorized
11	ForceAuth	Success	Authorized
12	ForceAuth	Success	Authorized
13	ForceAuth	Success	Authorized
14	ForceAuth	Success	Authorized
15	ForceAuth	Success	Authorized
16	ForceAuth	Success	Authorized
17	ForceAuth	Success	Authorized
18	ForceAuth	Success	Authorized
19	ForceAuth	Success	Authorized
20	ForceAuth	Success	Authorized
21	ForceAuth	Success	Authorized
22	ForceAuth	Success	Authorized
23	ForceAuth	Success	Authorized
24	ForceAuth	Success	Authorized
25	ForceAuth	Success	Authorized

Figure 7 - 19. Authenticator State window

This window displays the Authenticator State for individual ports on a selected device. A polling interval between *1s* and *60s* seconds can be set using the drop-down menu at the top of the window and clicking **OK**.

The information on this window is described as follows:

Parameter	Description
MAC Address	The MAC Address of the device of the corresponding index number.
Auth PAE State	The Authenticator PAE State value can be: Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, Force_Auth, Force_Unauth, or N/A. N/A (Not Available) indicates that the port's authenticator capability is disabled.
Backend State	The Backend Authentication State can be Request, Response, Success, Fail, Timeout, Idle, Initialize, or N/A. N/A (Not Available) indicates that the port's authenticator capability is disabled.
Port Status	Controlled Port Status can be Authorized, Unauthorized, or N/A.

Authenticator Statistics

This window contains the statistics objects for the Authenticator PAE associated with each port. An entry appears in this table for each port that supports the Authenticator function.

To view the Authenticator Statistics, click **Monitoring > Port Access Control > Authenticator Statistics**:

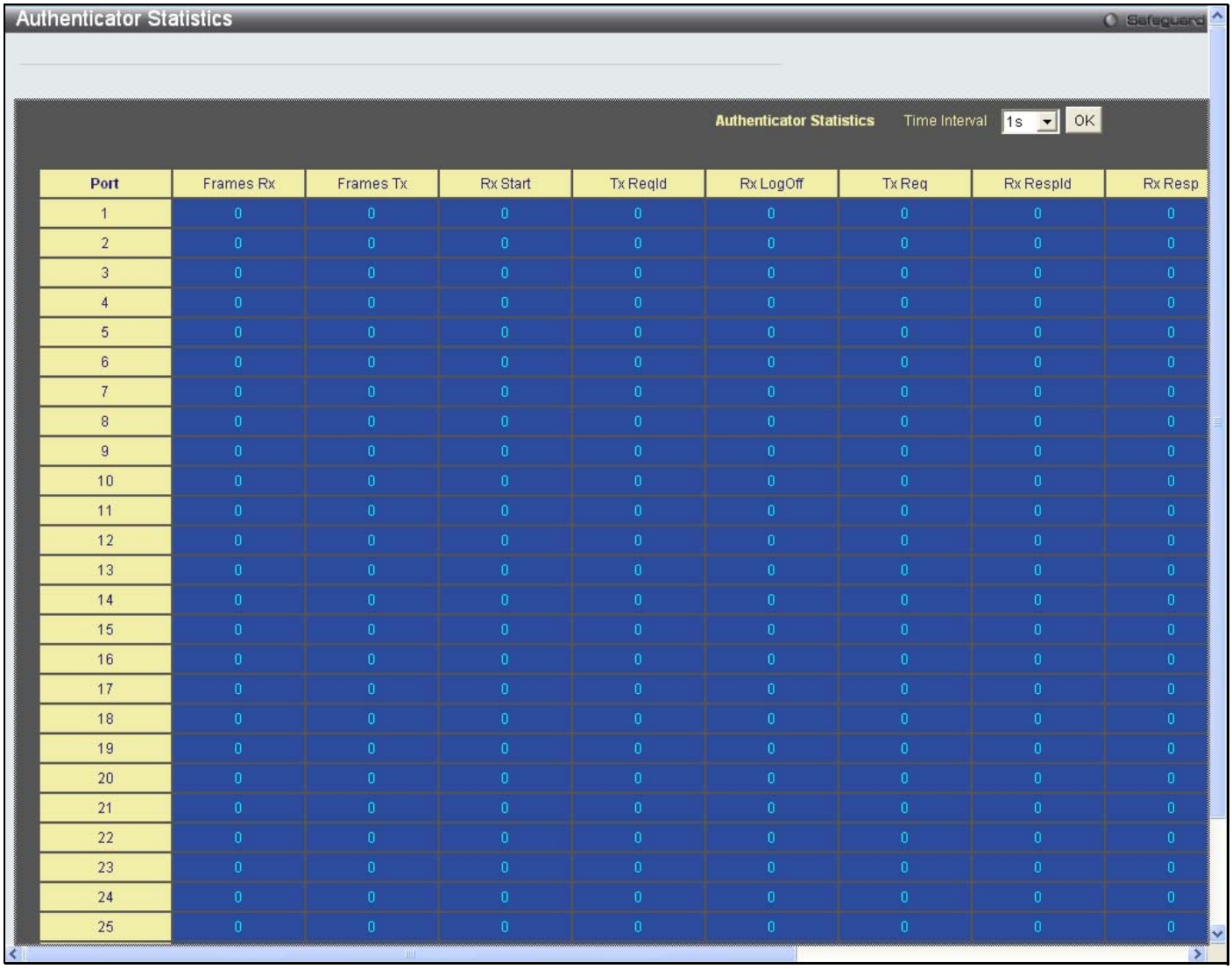


Figure 7 - 20. Authenticator Statistics window

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where “s” stands for seconds. The default value is one second.

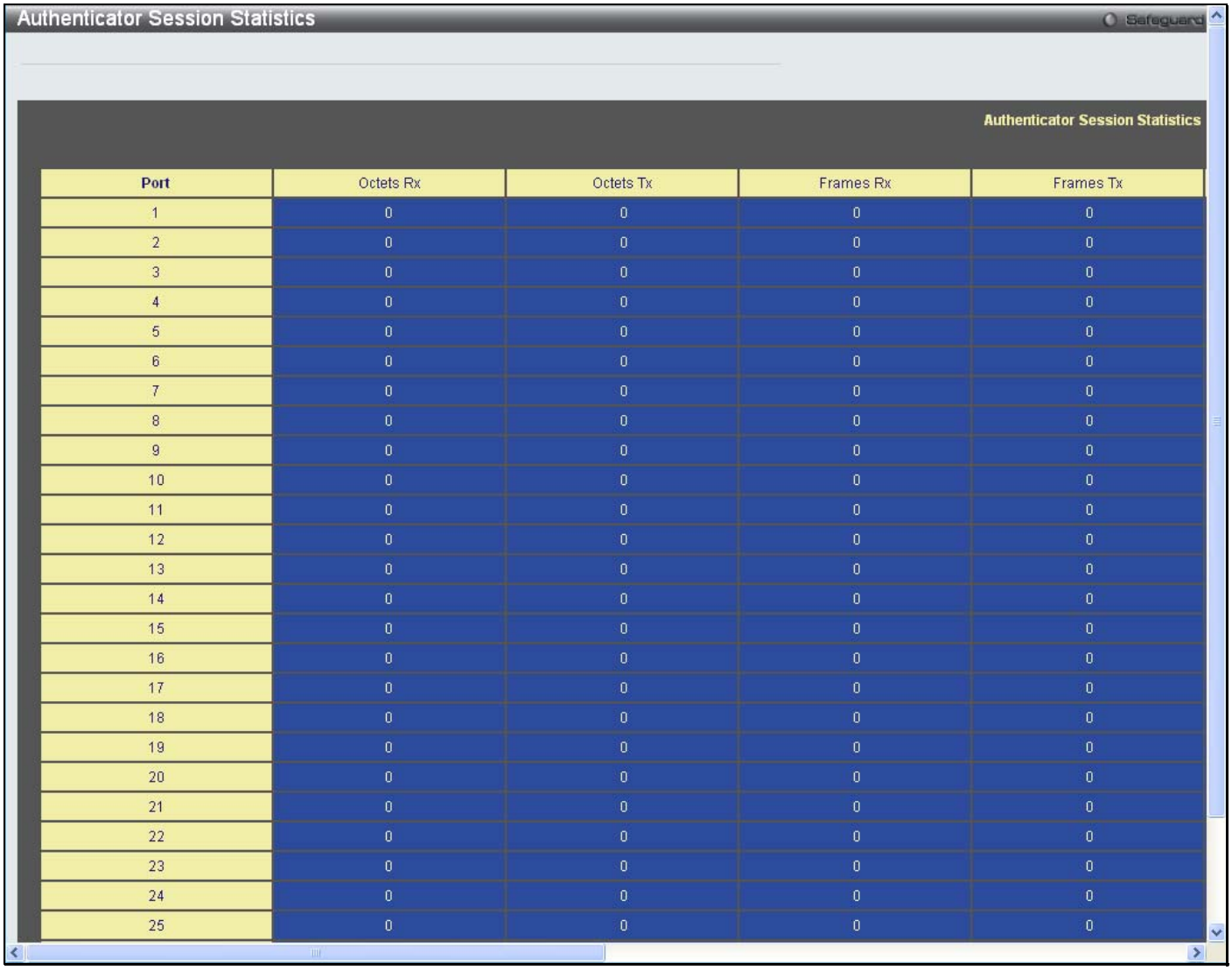
The following fields can be viewed:

Parameter	Description
Port	The identification number assigned to the Port by the System in which the Port resides.
Frames Rx	The number of valid EAPOL frames that have been received by this Authenticator.
Frames Tx	The number of EAPOL frames that have been transmitted by this Authenticator.
Rx Start	The number of EAPOL Start frames that have been received by this Authenticator.
TxReqId	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
RxLogOff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Tx Req	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
Rx RespId	The number of EAP Resp/Id frames that have been received by this Authenticator.
Rx Resp	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
Rx Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
Rx Error	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Last Version	The protocol version number carried in the most recently received EAPOL frame.
Last Source	The source MAC address carried in the most recently received EAPOL frame.

Authenticator Session Statistics

This window contains the session statistics objects for the Authenticator PAE associated with each port. An entry appears in this table for each port that supports the Authenticator function.

To view the **Authenticator Session Statistics** window, click **Monitoring > Port Access Control > Authenticator Session Statistics**:



Port	Octets Rx	Octets Tx	Frames Rx	Frames Tx
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0
23	0	0	0	0
24	0	0	0	0
25	0	0	0	0

Figure 7 - 21. Authenticator Session Statistics window

The user may select the desired time interval to update the statistics, between *1s* and *60s*, where “s” stands for seconds. The default value is one second.

The following fields can be viewed:

Parameter	Description
Port	The identification number assigned to the Port by the System in which the Port resides.
Octets Rx	The number of octets received in user data frames on this port during the session.
Octets Tx	The number of octets transmitted in user data frames on this port during the session.
Frames Rx	The number of user data frames received on this port during the session.
Frames Tx	The number of user data frames transmitted on this port during the session.
ID	A unique identifier for the session, in the form of a printable ASCII string of at least three characters.
Authentic Method	The authentication method used to establish the session. Valid Authentic Methods include: (1) Remote Authentic Server - The Authentication Server is external to the Authenticator’s System. (2) Local Authentic Server - The Authentication Server is located within the Authenticator’s System.
Time	The duration of the session in seconds.
Terminate Cause	The reason for the session termination. There are eight possible reasons for termination.

	1) Supplicant Logoff 2) Port Failure 3) Supplicant Restart 4) Reauthentication Failure 5) AuthControlledPortControl set to ForceUnauthorized 6) Port re-initialization 7) Port Administratively Disabled 8) Not Terminated Yet
UserName	The User-Name representing the identity of the Supplicant PAE.

Authenticator Diagnostics

This window contains the diagnostic information regarding the operation of the Authenticator associated with each port. An entry appears in this table for each port that supports the Authenticator function.

To view the **Authenticator Diagnostics** window, click **Monitoring > Port Access Control > Authenticator Diagnostics**:

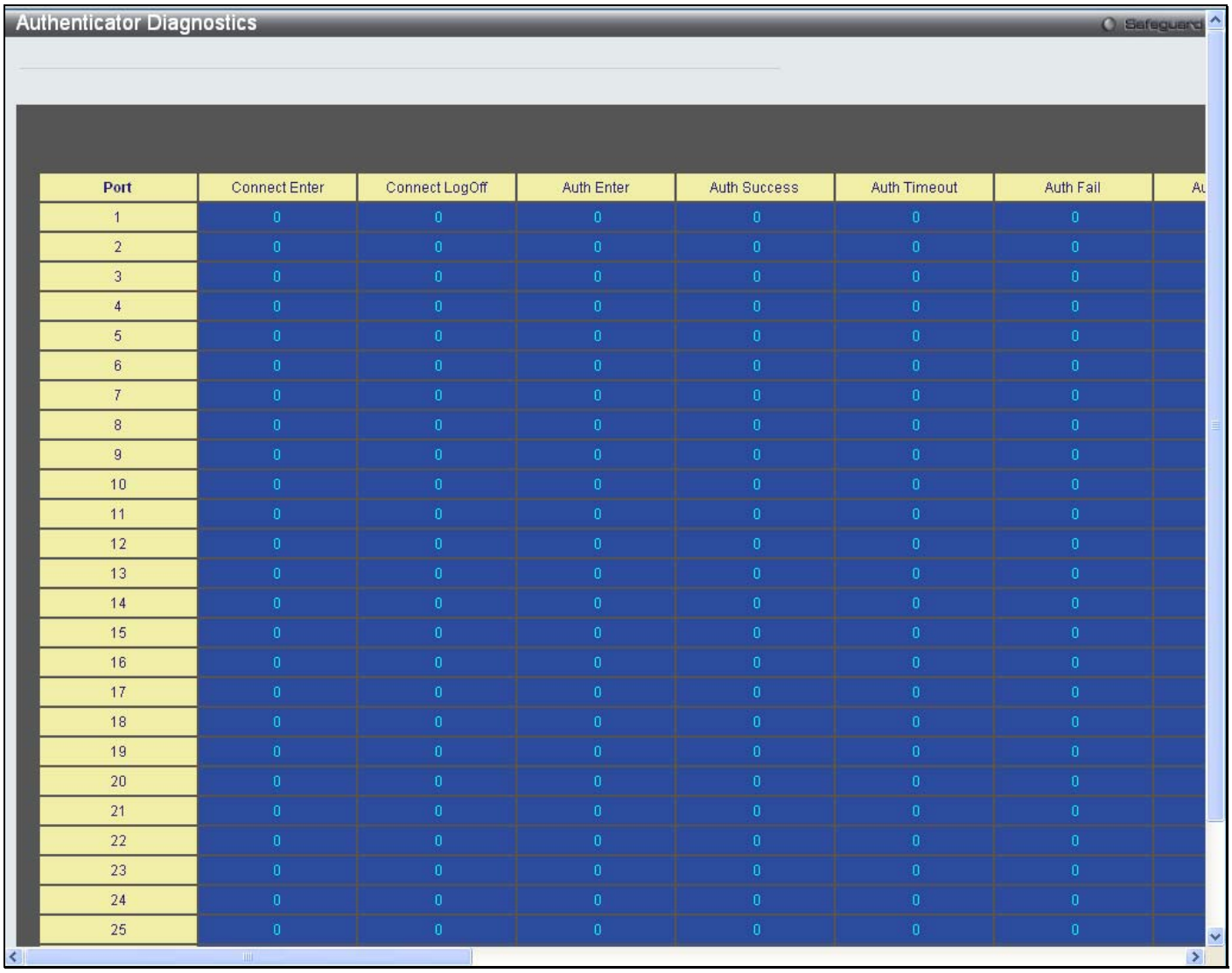


Figure 7 - 22. Authenticator Diagnostics window

The following fields can be viewed:

Parameter	Description
Port	The identification number assigned to the Port by the System in which the Port resides.
Connect Enter	Counts the number of times that the state machine transitions to the CONNECTING state from any other state.
Connect LogOff	Counts the number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message.
Auth Enter	Counts the number of times that the state machine transitions from CONNECTING to AUTHENTICATING, as a result of an EAP-Response/Identity message being received from the Supplicant.
Auth Success	Counts the number of times that the state machine transitions from AUTHENTICATING to AUTHENTICATED, as a result of the Backend Authentication state machine indicating successful authentication of the Supplicant (authSuccess = TRUE).
Auth Timeout	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout (authTimeout = TRUE).
Auth Fail	Counts the number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure (authFail = TRUE).
Auth Reauth	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a reauthentication request (reAuthenticate = TRUE).
Auth Start	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant.
Auth LogOff	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant.
Authed Reauth	Counts the number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a reauthentication request (reAuthenticate = TRUE).
Authed Start	Counts the number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of an EAPOL-Start message being received from the Supplicant.
Authed LogOff	Counts the number of times that the state machine transitions from AUTHENTICATED to DISCONNECTED, as a result of an EAPOL-Logoff message being received from the Supplicant.
Responses	Counts the number of times that the state machine sends an initial Access-Request packet to the Authentication server (i.e., executes sendRespToServer on entry to the RESPONSE state). Indicates that the Authenticator attempted communication with the Authentication Server.
AccessChallenges	Counts the number of times that the state machine receives an initial Access-Challenge packet from the Authentication server (i.e., aReq becomes TRUE, causing exit from the RESPONSE state). Indicates that the Authentication Server has communication with the Authenticator.
OtherReqToSupp	Counts the number of times that the state machine sends an EAP-Request packet (other than an Identity, Notification, Failure, or Success message) to the Supplicant (i.e., executes txReq on entry to the REQUEST state). Indicates that the Authenticator chose an EAP-method.
NonNakRespFromSup	Counts the number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK (i.e., rxResp becomes TRUE, causing the state machine to transition from REQUEST to RESPONSE, and the response is not an EAP-NAK). Indicates that the Supplicant can respond to the Authenticator's chosen EAP-method.
Bac Auth Success	Counts the number of times that the state machine receives an Accept message from the Authentication Server (i.e., aSuccess becomes TRUE, causing a transition from RESPONSE to SUCCESS). Indicates that the Supplicant has successfully authenticated to the Authentication Server.

Bac Auth Fail	Counts the number of times that the state machine receives a Reject message from the Authentication Server (i.e., aFail becomes TRUE, causing a transition from RESPONSE to FAIL). Indicates that the Supplicant has not authenticated to the Authentication Server.

Browse ARP Table

This window displays current ARP entries on the Switch. To search a specific ARP entry, enter an Interface Name or an IP Address at the top of the window and click **Find**. Click the **Show Static** button to display static ARP table entries. To clear the ARP Table, click **Clear All**.

The view this window, click **Monitoring > Browse ARP Table**:

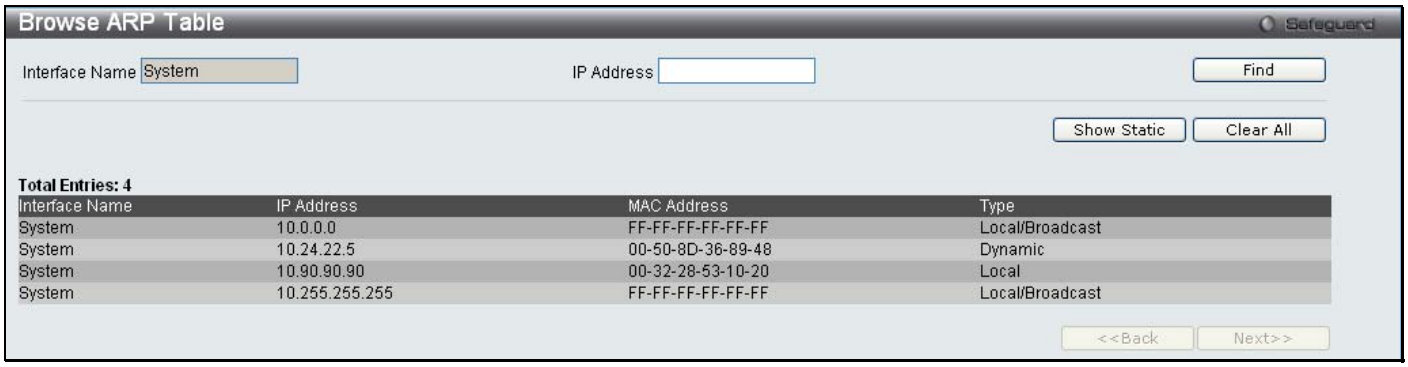


Figure 7 - 23. Browse ARP Table window

Browse VLAN

This window allows the VLAN status for each of the Switch's ports to be viewed by VLAN. Enter a VID (VLAN ID) in the field at the top of the window and click the **Find** button.

To view this window, click **Monitoring > Browse VLAN**:

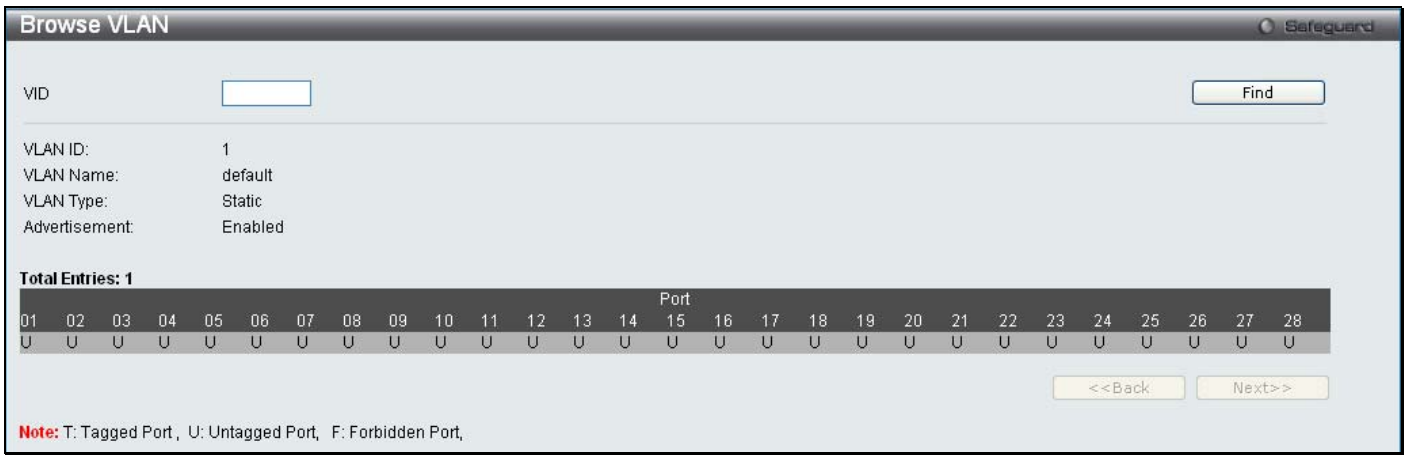

Browse VLAN
Safeguard
VID
Find
VLAN ID: 1
VLAN Name: default
VLAN Type: Static
Advertisement: Enabled
Total Entries: 1
Port
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
U U U U U U U U U U U U U U U U U U U U U U U U U U
<<Back
Next>>
Note: T: Tagged Port , U: Untagged Port, F: Forbidden Port,

Figure 7 - 24. Browse VLAN window

IGMP Snooping

The following windows are used to configure the IGMP Snooping settings of the Switch.

Browse IGMP Router Port

This window displays which of the Switch's ports are currently configured as router ports. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by S. A router port that is dynamically configured by the Switch is designated by D, while a Forbidden port is designated by F. Enter a VID (VLAN ID) in the field at the top of the window and click the **Find** button to display the various types of IGMP router ports that belong to the specified VLAN.

To view this window, click **Monitoring > IGMP Snooping > Browse IGMP Router Port**:

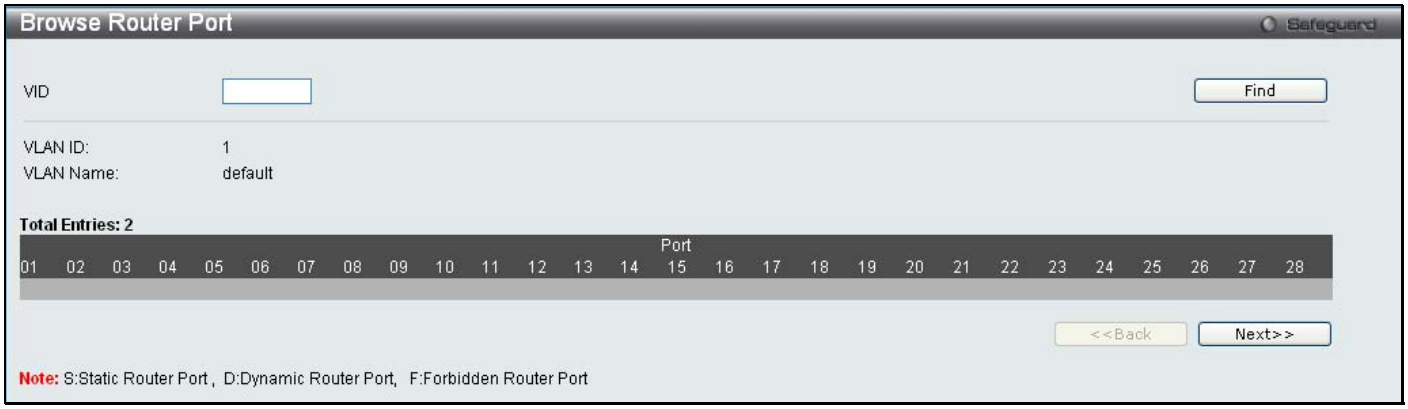

Browse Router Port
Safeguard
VID
Find
VLAN ID: 1
VLAN Name: default
Total Entries: 2
Port
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
<<Back
Next>>
Note: S:Static Router Port , D:Dynamic Router Port, F:Forbidden Router Port

Figure 7 - 25. Browse Router Port window

IGMP Snooping Group

This window allows the Switch's IGMP Snooping Group Table to be searched. IGMP snooping allows the Switch to read the Multicast Group IP address and source IP address from IGMP packets that pass through the Switch. The number of IGMP reports that are snooped are displayed in the Reports field.

To view this window, click **Monitoring > IGMP Snooping > IGMP Snooping Group**:

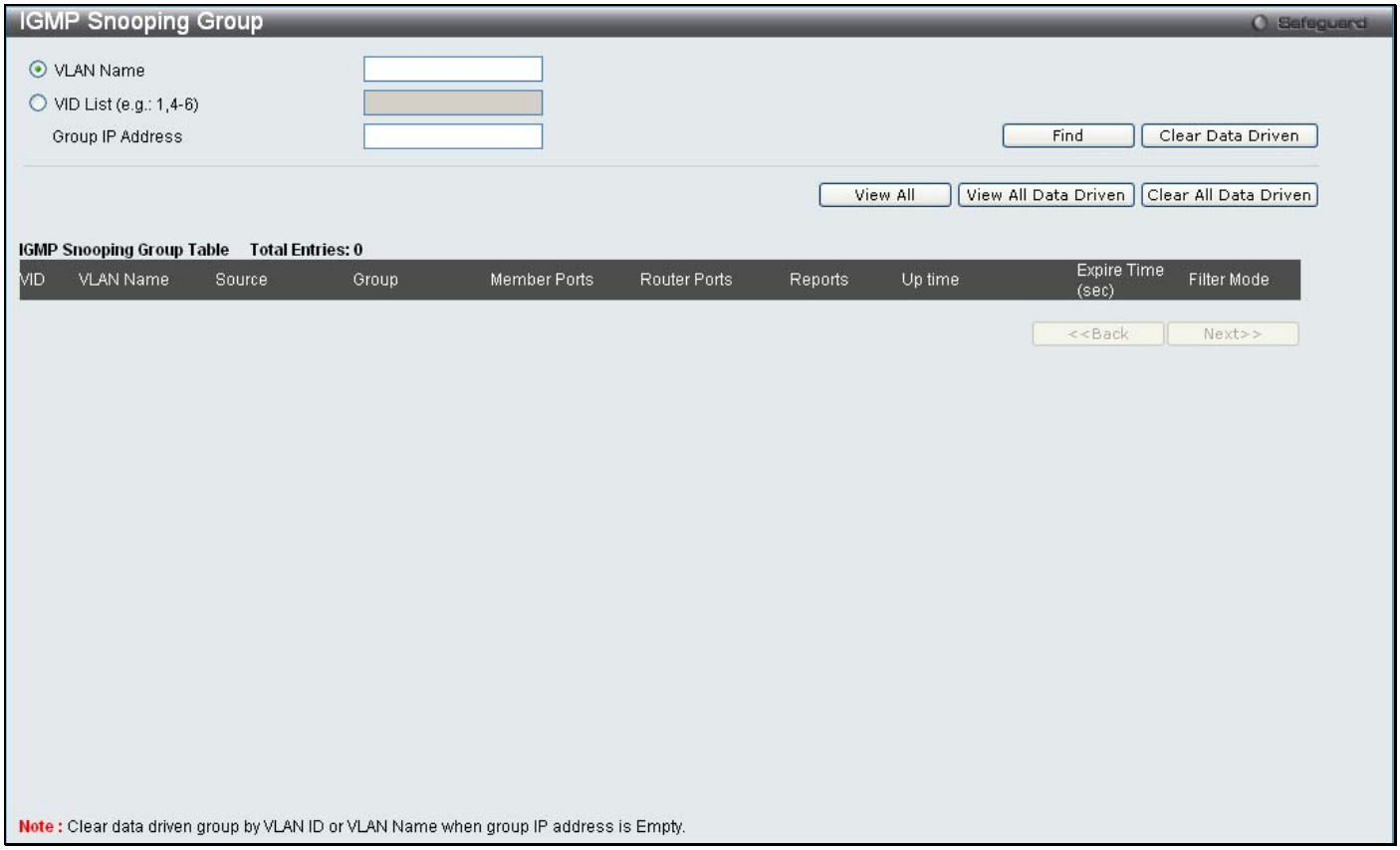

IGMP Snooping Group
Safeguard
VLAN Name
VID List (e.g.: 1,4-6)
Group IP Address
Find
Clear Data Driven
View All
View All Data Driven
Clear All Data Driven
IGMP Snooping Group Table Total Entries: 0
VID VLAN Name Source Group Member Ports Router Ports Reports Up time Expire Time (sec) Filter Mode
<<Back
Next>>
Note : Clear data driven group by VLAN ID or VLAN Name when group IP address is Empty.

Figure 7 - 26. IGMP Snooping Group window

The following fields can be searched:

Parameter	Description
VLAN Name	The VLAN ID of the multicast group.
VID List (e.g.: 1, 4-6)	The VLAN ports of the multicast group.
Group IP Address	The IP address of the multicast group.

Enter the appropriate information and click **Find**. The searched entries will be shown in the IGMP Snooping Group Table. Click **View All** to see all the entries.

Click **View All Data Driven** to display all the data driven groups learned in the IGMP Snooping Group Table.

Click **Clear Data Driven** to clear the specific data driven groups learned in IGMP Snooping Group Table.

Click **Clear All Data Driven** to clear all data driven groups learned in IGMP Snooping Group Table.

NOTE: To configure IGMP snooping for the Switch, go to the **L2 Features** folder and select **IGMP Snooping > IGMP Snooping Settings**.

IGMP Snooping Host

This window displays current IGMP Snooping host information on the Switch.

To view this window, click **Monitoring > IGMP Snooping > IGMP Snooping Host**:

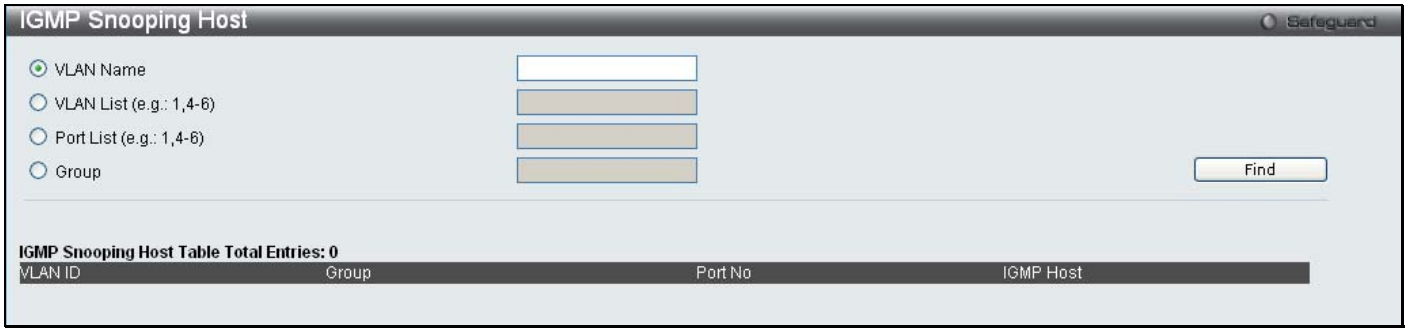


Figure 7 - 27. IGMP Snooping Host window

Click the corresponding radio button, enter the VLAN Name, VLAN List, Port List, or the Group to view IGMP snooping host information, and click **Find**. The searched entries will be displayed in the lower half of the window.

MLD Snooping

Browse MLD Router Port

This window displays which of the Switch's ports are currently configured as router ports in IPv6. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by S. A router port that is dynamically configured by the Switch and is designated by D, whereas a Forbidden port is designated by F. Enter a VID (VLAN ID) in the field at the top of the window and click the **Find** button to display the various types of MLD router ports that beliong to the specified VLAN.

To view this window, click **Monitoring > MLD Snooping > Browse MLD Router Port**:

Browse MLD Router Port
Safeguard
VID
Find
VLAN ID: 1
VLAN Name: default
Total Entries: 1
Port
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
<<Back
Next>>
Note: S:Static Router Port , D:Dynamic Router Port, F:Forbidden Router Port

Figure 7 - 28. Browse MLD Router Port window

MLD Snooping Group

The following window allows the user to view MLD Snooping Groups present on the Switch. MLD Snooping is an IPv6 function comparable to IGMP Snooping for IPv4. The user may browse this table by VLAN present in the Switch by entering that VLAN Name in the empty field shown below, and clicking the **Find** button.

To view this window, click **Monitoring > MLD Snooping > MLD Snooping Group**:

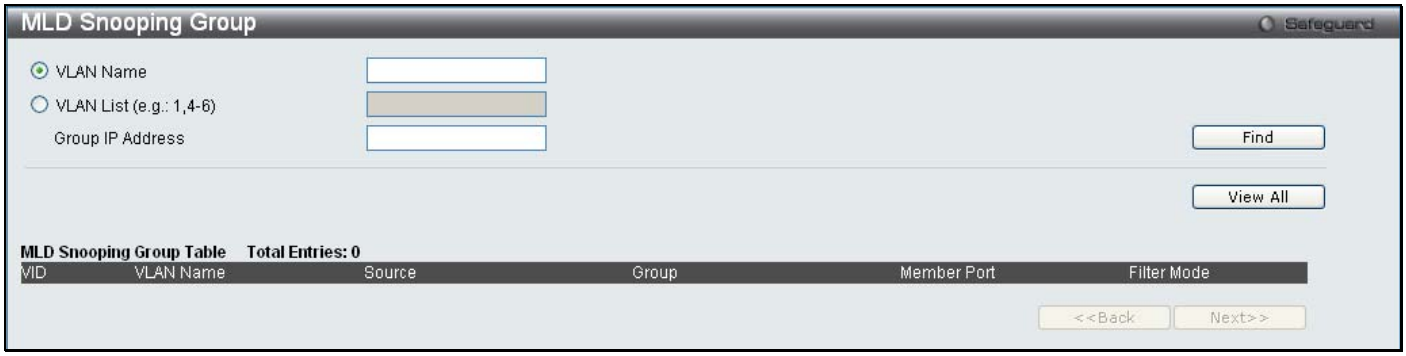


Figure 7 - 29. MLD Snooping Group window

Enter a VLAN Name or VLAN List and Group IP Address in the appropriate field and click the **Find** button.

The searched entries will be shown in the MLD Snooping Group Table. Click **View All** to see all the entries.

LLDP

The Switch offers three LLDP statistic windows.

LLDP Statistics System

To view this window, click **Monitoring > LLDP > LLDP Statistics System**:

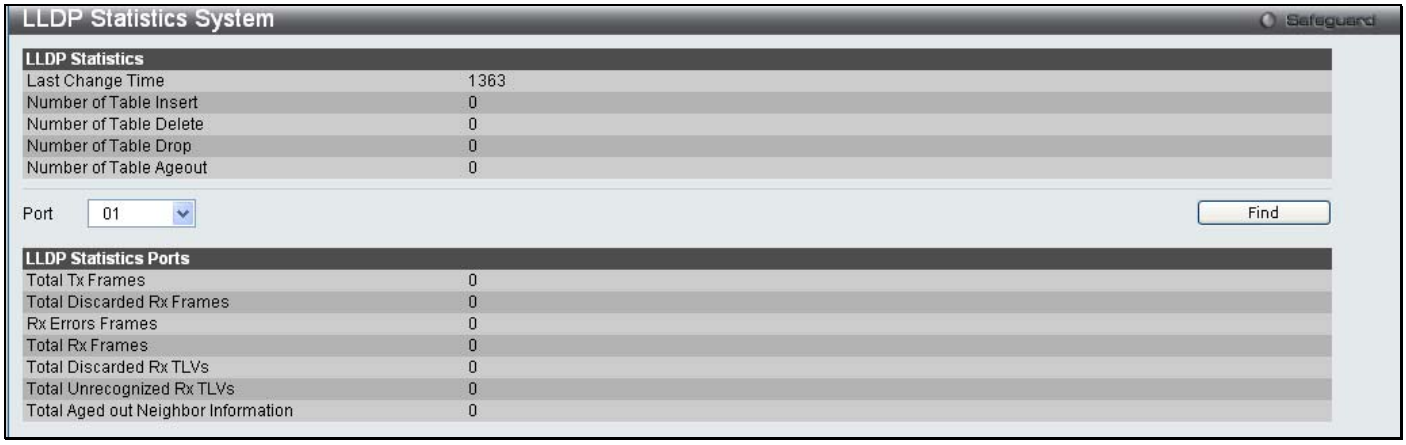


Figure 7 - 30. LLDP Statistics System window

LLDP Local Port Information

To view this window, click **Monitoring > LLDP > LLDP Local Port Information**:

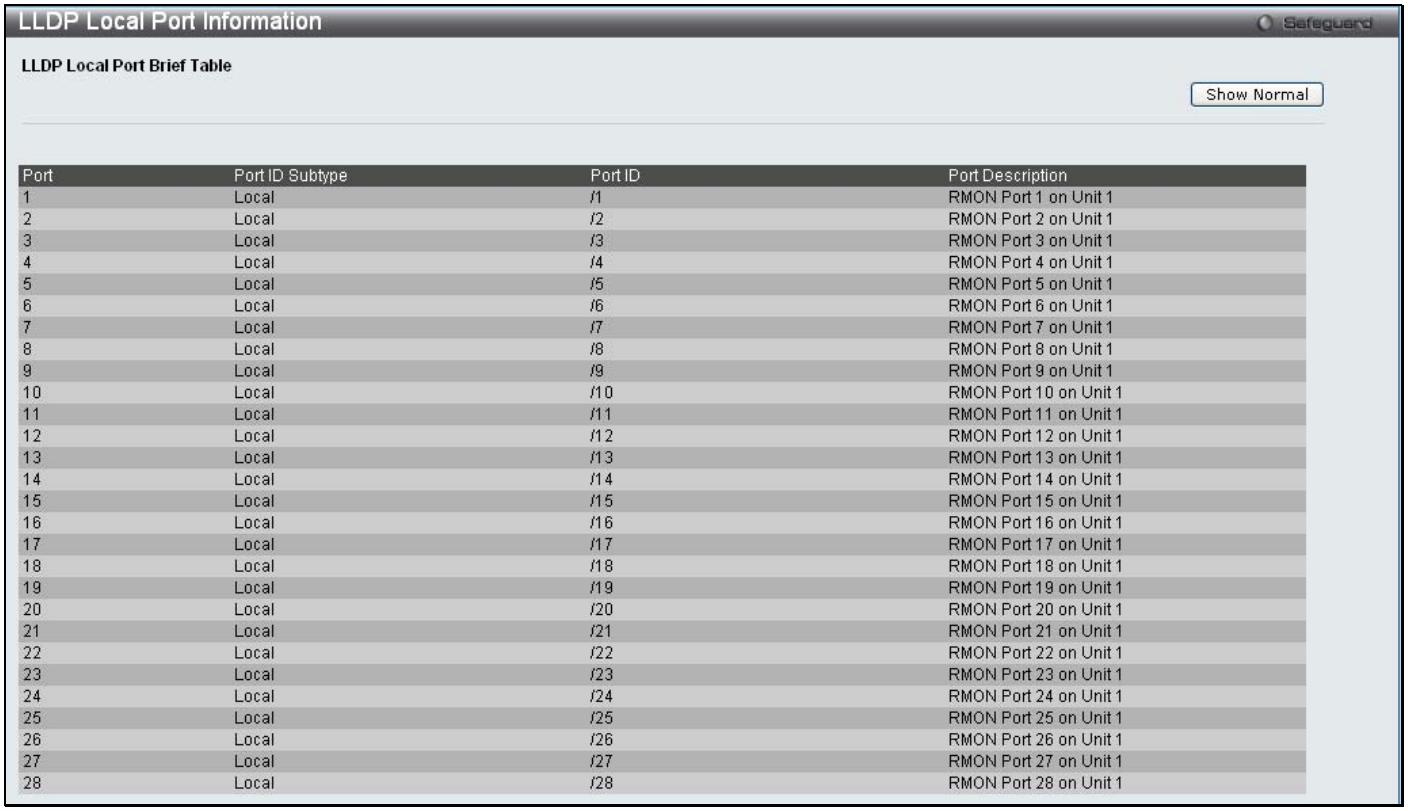

LLDP Local Port Information
Safeguard
LLDP Local Port Brief Table
Show Normal
Port Port ID Subtype Port ID Port Description
1 Local /1 RMON Port 1 on Unit 1
2 Local /2 RMON Port 2 on Unit 1
3 Local /3 RMON Port 3 on Unit 1
4 Local /4 RMON Port 4 on Unit 1
5 Local /5 RMON Port 5 on Unit 1
6 Local /6 RMON Port 6 on Unit 1
7 Local /7 RMON Port 7 on Unit 1
8 Local /8 RMON Port 8 on Unit 1
9 Local /9 RMON Port 9 on Unit 1
10 Local /10 RMON Port 10 on Unit 1
11 Local /11 RMON Port 11 on Unit 1
12 Local /12 RMON Port 12 on Unit 1
13 Local /13 RMON Port 13 on Unit 1
14 Local /14 RMON Port 14 on Unit 1
15 Local /15 RMON Port 15 on Unit 1
16 Local /16 RMON Port 16 on Unit 1
17 Local /17 RMON Port 17 on Unit 1
18 Local /18 RMON Port 18 on Unit 1
19 Local /19 RMON Port 19 on Unit 1
20 Local /20 RMON Port 20 on Unit 1
21 Local /21 RMON Port 21 on Unit 1
22 Local /22 RMON Port 22 on Unit 1
23 Local /23 RMON Port 23 on Unit 1
24 Local /24 RMON Port 24 on Unit 1
25 Local /25 RMON Port 25 on Unit 1
26 Local /26 RMON Port 26 on Unit 1
27 Local /27 RMON Port 27 on Unit 1
28 Local /28 RMON Port 28 on Unit 1

Figure 7 - 31. LLDP Local Port Information window

LLDP Remote Port Information

To view this window, click **Monitoring > LLDP > LLDP Remote Port Information**:

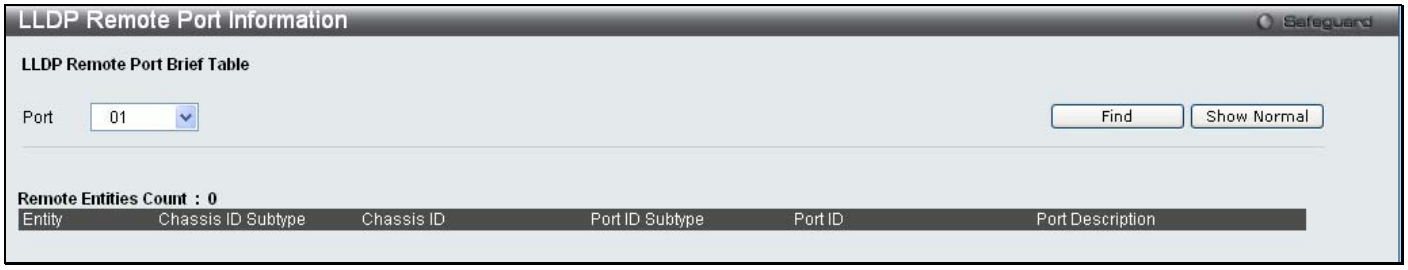

LLDP Remote Port Information
Safeguard
LLDP Remote Port Brief Table
Port 01
Find
Show Normal
Remote Entities Count : 0
Entity Chassis ID Subtype Chassis ID Port ID Subtype Port ID Port Description

Figure 7 - 32. LLDP Remote Port Information window

MBA Authentication State

This window allows the user to view the MAC-based Access Control authentication information. Specify the port list to view and click **Find**. To remove an entry, enter the appropriate information and click **Clear By Port**. Click **View All Hosts** to see all the entries. To remove all hosts, click **Clear All Hosts**.

To view this window, click **Monitoring > MBA Authentication State**:

Figure 7 - 33. MBA Authentication State window

Browse Session Table

This window displays the management sessions since the Switch was last rebooted.

To view the **Browse Session Table** window, click **Monitoring > Browse Session Table**:

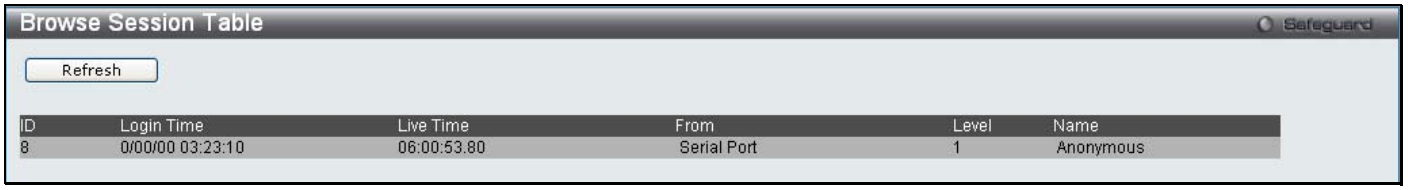


Figure 7 - 34. Browse Session Table window

MAC Address Table

This allows the Switch's dynamic MAC address forwarding table to be viewed. When the Switch learns an association between a MAC address and a port number, it makes an entry into its forwarding table. These entries are then used to forward packets through the Switch.

To view the **MAC Address Table** window, click **Monitoring > MAC Address Table**

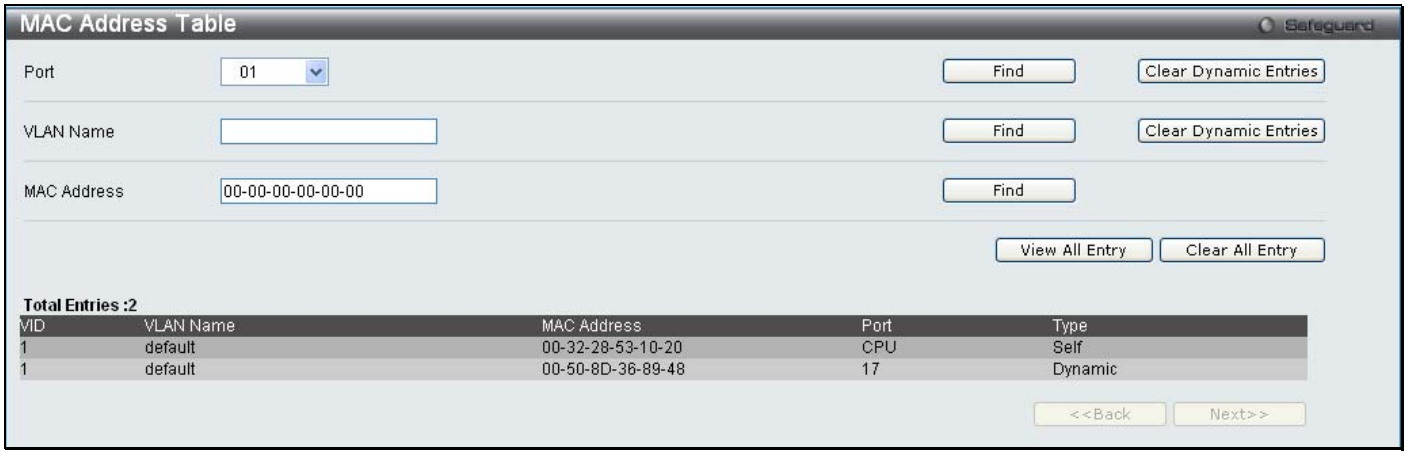


Figure 7 - 35. MAC Address Table window

The functions used in the MAC address table are described below:

Parameter	Description
Port	The port to which the MAC address below corresponds.
VLAN Name	Enter a VLAN Name for the forwarding table to be browsed by.

MAC Address	Enter a MAC address for the forwarding table to be browsed by.
Find	Allows the user to move to a sector of the database corresponding to a user defined port, VLAN, or MAC address.
Clear Dynamic Entries	Click this button will allow the user to delete all dynamic entries of the address table.
View All Entry	Click this button will allow the user to view all entries of the address table.
Clear All Entry	Click this button will allow the user to delete all entries of the address table.

System Log

The web manager allows the Switch's history log, as compiled by the Switch's management agent, to be viewed.

To view the Switch history log, click **Monitoring > System Log**:

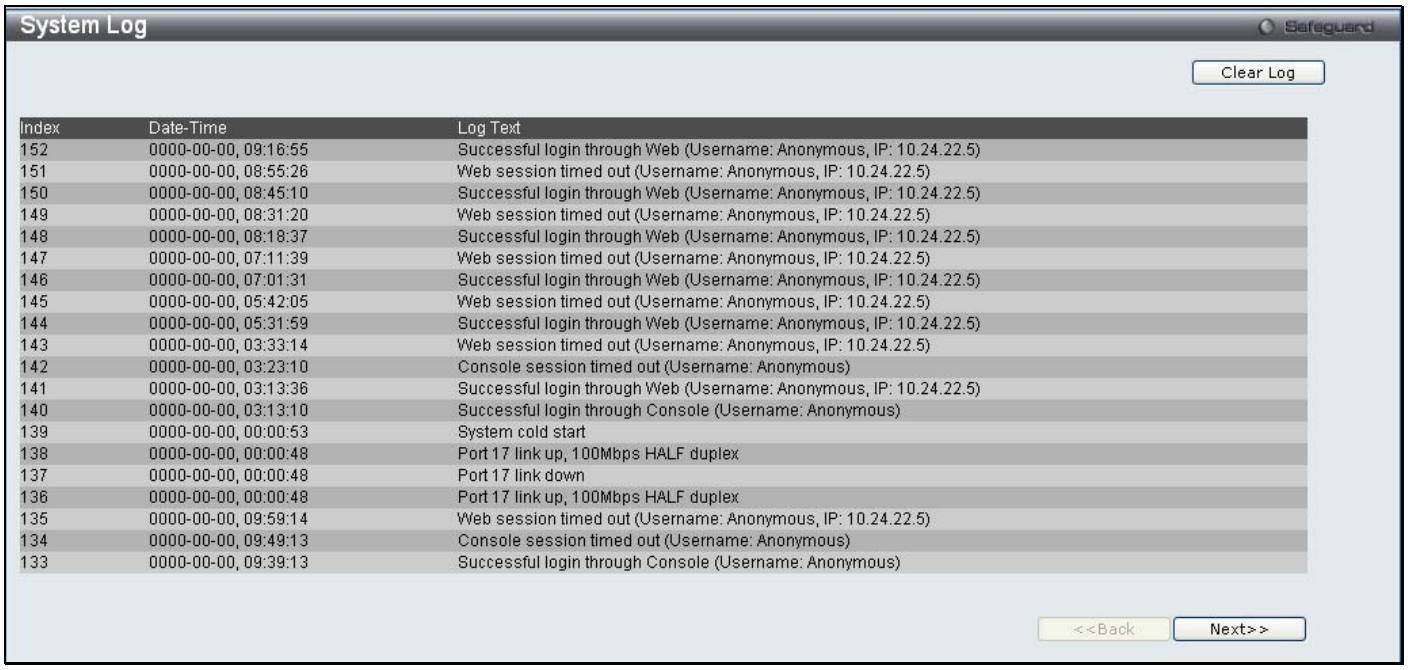

System Log
Safeguard
Clear Log
Index
Date-Time
Log Text
152 0000-00-00, 09:16:55 Successful login through Web (Username: Anonymous, IP: 10.24.22.5)
151 0000-00-00, 08:55:26 Web session timed out (Username: Anonymous, IP: 10.24.22.5)
150 0000-00-00, 08:45:10 Successful login through Web (Username: Anonymous, IP: 10.24.22.5)
149 0000-00-00, 08:31:20 Web session timed out (Username: Anonymous, IP: 10.24.22.5)
148 0000-00-00, 08:18:37 Successful login through Web (Username: Anonymous, IP: 10.24.22.5)
147 0000-00-00, 07:11:39 Web session timed out (Username: Anonymous, IP: 10.24.22.5)
146 0000-00-00, 07:01:31 Successful login through Web (Username: Anonymous, IP: 10.24.22.5)
145 0000-00-00, 05:42:05 Web session timed out (Username: Anonymous, IP: 10.24.22.5)
144 0000-00-00, 05:31:59 Successful login through Web (Username: Anonymous, IP: 10.24.22.5)
143 0000-00-00, 03:33:14 Web session timed out (Username: Anonymous, IP: 10.24.22.5)
142 0000-00-00, 03:23:10 Console session timed out (Username: Anonymous)
141 0000-00-00, 03:13:36 Successful login through Web (Username: Anonymous, IP: 10.24.22.5)
140 0000-00-00, 03:13:10 Successful login through Console (Username: Anonymous)
139 0000-00-00, 00:00:53 System cold start
138 0000-00-00, 00:00:48 Port 17 link up, 100Mbps HALF duplex
137 0000-00-00, 00:00:48 Port 17 link down
136 0000-00-00, 00:00:48 Port 17 link up, 100Mbps HALF duplex
135 0000-00-00, 09:59:14 Web session timed out (Username: Anonymous, IP: 10.24.22.5)
134 0000-00-00, 09:49:13 Console session timed out (Username: Anonymous)
133 0000-00-00, 09:39:13 Successful login through Console (Username: Anonymous)
<<Back
Next>>

Figure 7 - 36. System Log window

The Switch can record event information in its own logs. Click **Next** to go to the next page of the **System Log** window. Clicking **Clear** will allow the user to clear the Switch History Log.

The information in the table is categorized as:

Parameter	Description
Index	A counter incremented whenever an entry to the Switch's history log is made. The table displays the last entry (highest sequence number) first.
Date-Time	Displays the time in days, hours, minutes, and seconds since the Switch was last restarted.
Log Text	Displays text describing the event that triggered the history log entry.

Section 8

Save and Tools

Save Configuration

Save Log

Save All

Configuration File Upload & Download

Upload Log File

Reset

Ping Test

Download Firmware

Reboot System

The three **Save** windows include: **Save Configuration**, **Save Log**, and **Save All**. Each version of the window will aid the user in saving configurations to the Switch's memory.

The options include:

- **Save Configuration** to save the current configuration file.
- **Save Log** to save only the current log.
- **Save All** to save the current configuration file and log.

Save Configuration

Open the **Save** drop-down menu at the top of the Web manager and click **Save Configuration** to open the following window:

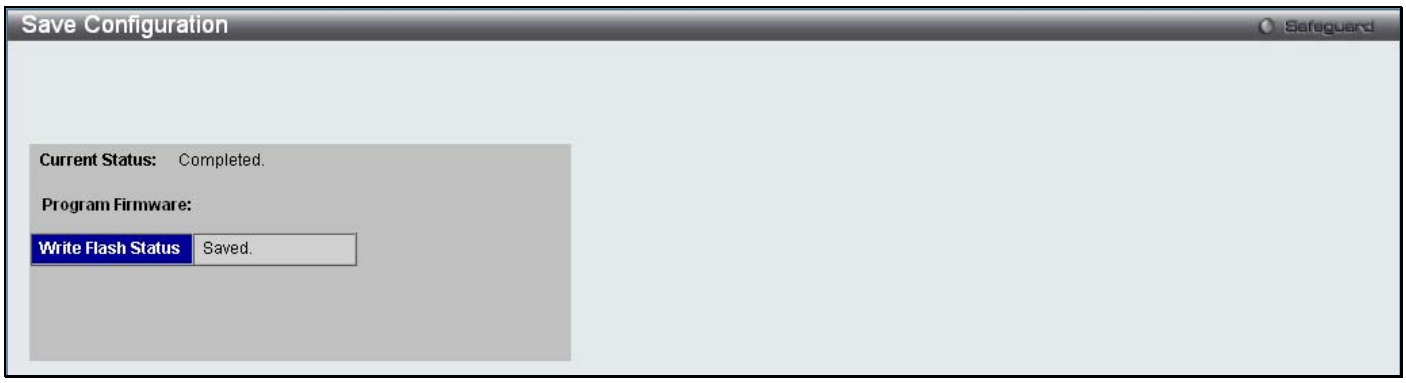


Figure 8 - 1. Save Configuration window

Save Log

Open the **Save** drop-down menu at the top of the Web manager and click **Save Log** to open the following window:

Figure 8 - 2. Save Log window

Save All

Open the **Save** drop-down menu at the top of the Web manager and click **Save All** to open the following window:

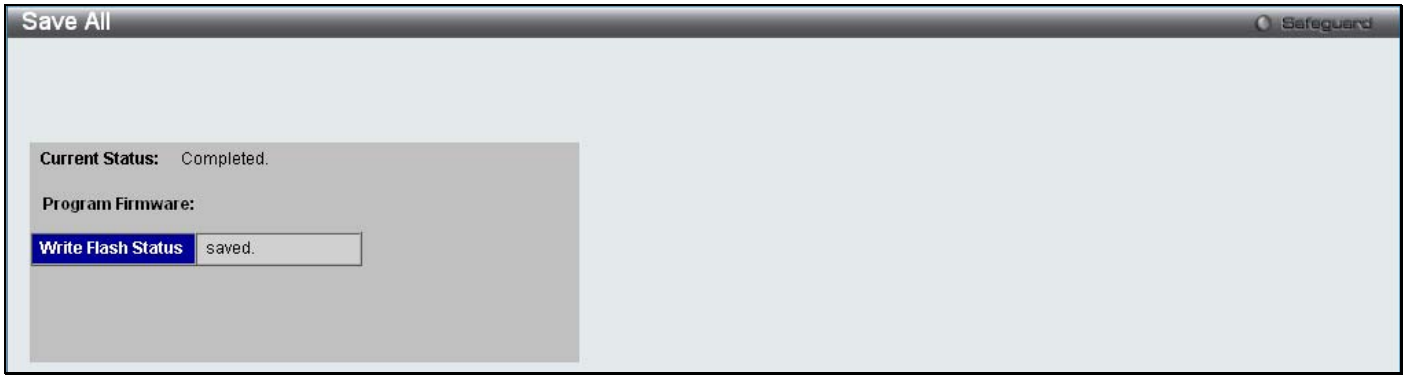


Figure 8 - 3. Save All window

Configuration File Upload & Download

The Switch can upload and download configuration files.

Open the **Tools** drop-down menu on the left-hand side of the menu bar at the top of the Web manager and click **Configuration File Upload & Download** to open the following window:

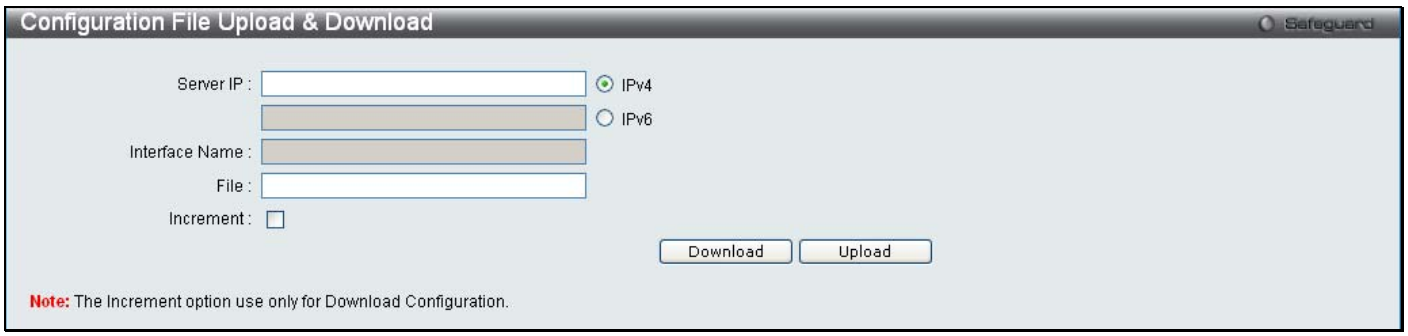


Figure 8 - 4. Configuration File Upload & Download window

Use the radio button to select IPv4 and specify File name or use the radio button to select IPv6, enter a Server IP, Interface Name, and File name. Click either **Download** or **Upload** to initiate the file transfer.

Upload Log File

To upload a log file, enter a Server IP address, use the radio button to select IPv4 and then enter a File name, or use the radio button to select IPv6, enter a Server IP, Interface Name, and File name. Click **Upload**.

Open the **Tools** drop-down menu on the left-hand side of the menu bar at the top of the Web manager and click **Upload Log File** to open the following window:

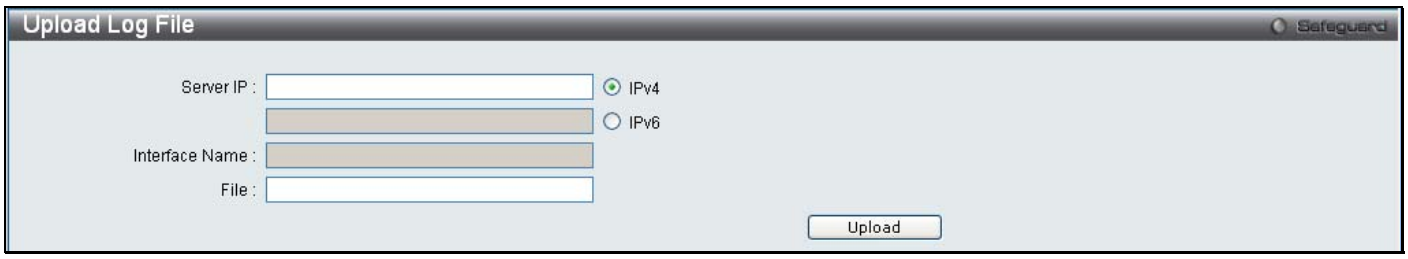


Figure 8 - 5. Upload Log File window

Reset

The Reset function has several options when resetting the Switch. Some of the current configuration parameters can be retained while resetting all other configuration parameters to their factory defaults.

NOTE: Only the Reset System option will enter the factory default parameters into the Switch's non-volatile RAM, and then restart the Switch. All other options enter the factory defaults into the current configuration, but do not save this configuration. Reset System will return the Switch's configuration to the state it was when it left the factory

NOTE: The serial port's baud rate will not be changed by the reset command. It will not be restored to the factory default setting.

Reset gives the option of retaining the Switch's User Accounts and History Log while resetting all other configuration parameters to their factory defaults. If the Switch is reset using this window, and **Save Changes** is not executed, the Switch will return to the last saved configuration when rebooted.

Open the **Tools** drop-down menu on the left-hand side of the menu bar at the top of the Web manager and click **Reset System** to open the following window:

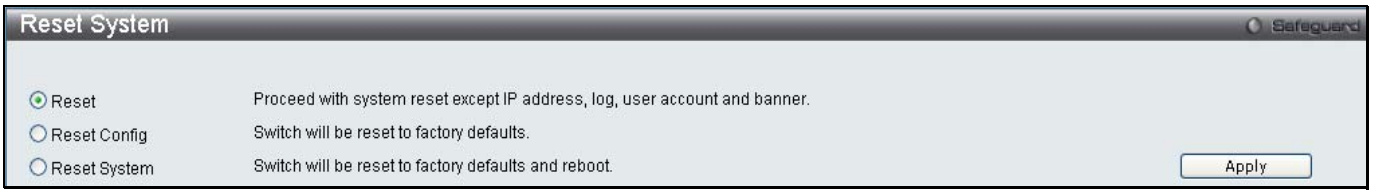

Reset System
Safeguard
Reset
Proceed with system reset except IP address, log, user account and banner.
Reset Config
Switch will be reset to factory defaults.
Reset System
Switch will be reset to factory defaults and reboot.
Apply

Figure 8 - 6. Reset System window

Ping Test

Users can Ping either an IPv4 address or an IPv6 address. Ping is a small program that sends ICMP Echo packets to the IP address you specify. The destination node then responds to or “echoes” the packets sent from the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

Open the **Tools** drop-down menu on the left-hand side of the menu bar at the top of the Web manager and click **Ping Test** to open the following window:

Figure 8 - 7. Ping Test window

The user may click the Infinite times radio button, in the Repeat Pinging for field, which will tell the ping program to keep sending ICMP Echo packets to the specified IP address until the program is stopped. The user may opt to choose a specific number of times to ping the Target IP Address by clicking its radio button and entering a number between *1* and *255*. Click **Start** to initiate the Ping program.

The following parameters may be configured or viewed:

Parameter	Description
Target IP Address	Enter an IP address to be Pinged.
Interface Name	For IPv6 only, enter the name of the interface to be Pinged.
Repeat Pinging for	Enter the number of times desired to attempt to Ping either the IPv4 address or the IPv6 address configured in this window. Users may enter a number of times between *1* and *255*.
Size	For IPv6 only, enter a value between *1* and *6000*. The default is *100*.
Timeout	For IPv4, select a timeout period between *1* and *99* seconds for this Ping message to reach its destination. For IPv6, select a timeout period between *1* and *10* seconds for this Ping message to reach its destination. In either case, if the packet fails to find the IP address in this specified time, the Ping packet will be dropped.

Click **Start** to initialize the Ping program

Download Firmware

The Switch supports dual image storage for firmware file backup and restoration. The firmware images are indexed by ID number 1 or 2. To change the boot firmware image, use the Image ID drop-down menu to select the desired firmware file to backup or restore. The default Switch settings will use image ID 1 as the boot firmware file.

Open the **Tools** drop-down menu on the left-hand side of the menu bar at the top of the Web manager and click **Download Firmware** to open the following window:

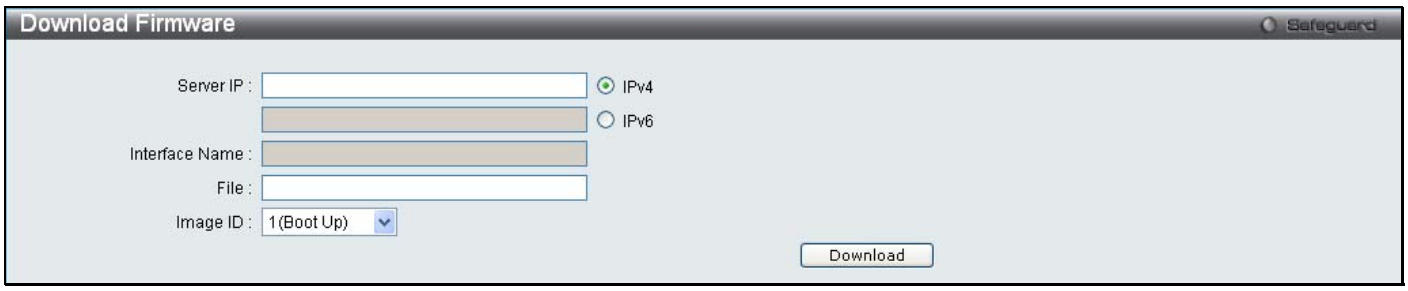


Figure 8 - 8. Download Firmware window

Use the radio button to select either IPv4 or IPv6. Enter the TFTP Server IP address for the type of IP selected. Specify the path/file name of the TFTP File. Select the desired Image ID, *1(Boot Up)* or *2*. Click **Download** to initiate the file transfer.

Reboot System

The following window is used to restart the Switch.

Reboot System
Safeguard
Do you want to save the settings ?
Yes
No
Reboot
If you do not save the settings, all changes made in this session will be lost.

Figure 8 - 9. Reboot System window

Clicking the Yes radio button will instruct the Switch to save the current configuration to non-volatile RAM before restarting the Switch.

Clicking the No radio button instructs the Switch not to save the current configuration before restarting the Switch. All of the configuration information entered from the last time **Save Changes** was executed will be lost.

Click the **Reboot** button to restart the Switch.

Appendix A

Mitigating ARP Spoofing Attacks Using Packet Content ACL

Address Resolution Protocol (ARP) is the standard method for finding a host's hardware address (MAC address) when only its IP address is known. This protocol is vulnerable because it can spoof the IP and MAC information in the ARP packets to attack a LAN (known as ARP spoofing). This document is intended to introduce ARP protocol, ARP spoofing attacks, and the counter measure brought by D-Link's switches to counter the ARP spoofing attack.

- **How Address Resolution Protocol works**

In the process of ARP, PC A will, firstly, issue an ARP request to query PC B's MAC address. The network structure is shown in Figure-1.

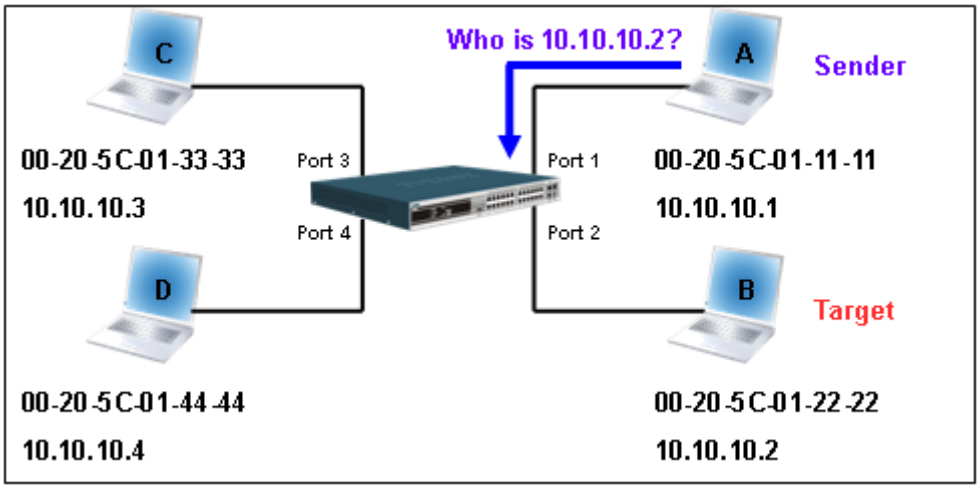


Figure-1

In the mean time, PC A's MAC address will be written into the "Sender H/W Address" and its IP address will be written into the "Sender Protocol Address" in ARP payload. As PC B's MAC address is unknown, the "Target H/W Address" will be "00-00-00-00-00-00" while PC B's IP address will be written into the "Target Protocol Address", shown in Table-1.

H/W type	Protocol type	H/W address length	Protocol address length	Operation	Sender H/W address	Sender protocol address	Target H/W address	Target protocol address
				ARP request	00-20-5C-01-11-11	***10.10.10.1***	***00-00-00-00-00-00***	***10.10.10.2***

Table -1 (ARP Payload)

The ARP request will be encapsulated into Ethernet frame and sent out. As can be seen in Table-2, the "Source Address" in the Ethernet frame will be PC A's MAC address. Since an ARP request is sent via a broadcast, the "Destination address" is in the format of an Ethernet broadcast (FF-FF-FF-FF-FF-FF).

Destination	Source address	Ether-type	ARP	FCS

address				
FF-FF-FF-FF-FF-FF	***00-20-5C-01-11-11***			

Table-2 (Ethernet frame format)

When the switch receives the frame, it will check the “Source Address” in the Ethernet frame’s header. If the address is not in its Forwarding Table, the switch will learn PC A’s MAC and the associated port into its Forwarding Table.

Forwarding Table

Port1 00-20-5C-01-11-11

In addition, when the switch receives the broadcast ARP request, it will flood the frame to all ports except the source port, port 1 (see Figure -2).

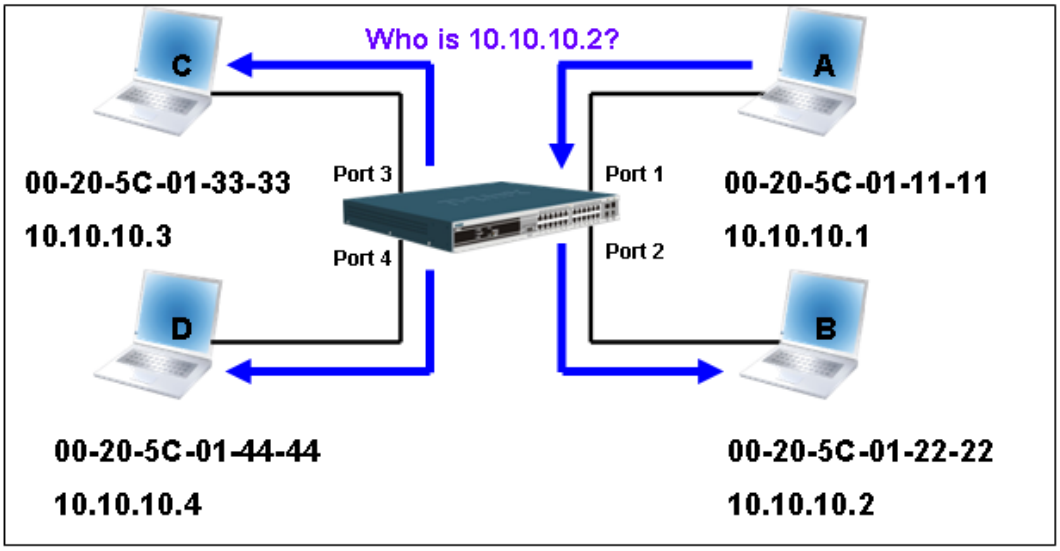


Figure - 2

When the switch floods the frame of ARP requests to the network, all PCs will receive and examine the frame but only PC B will reply to the query as the destination IP address of PC B matches (see Figure-3).

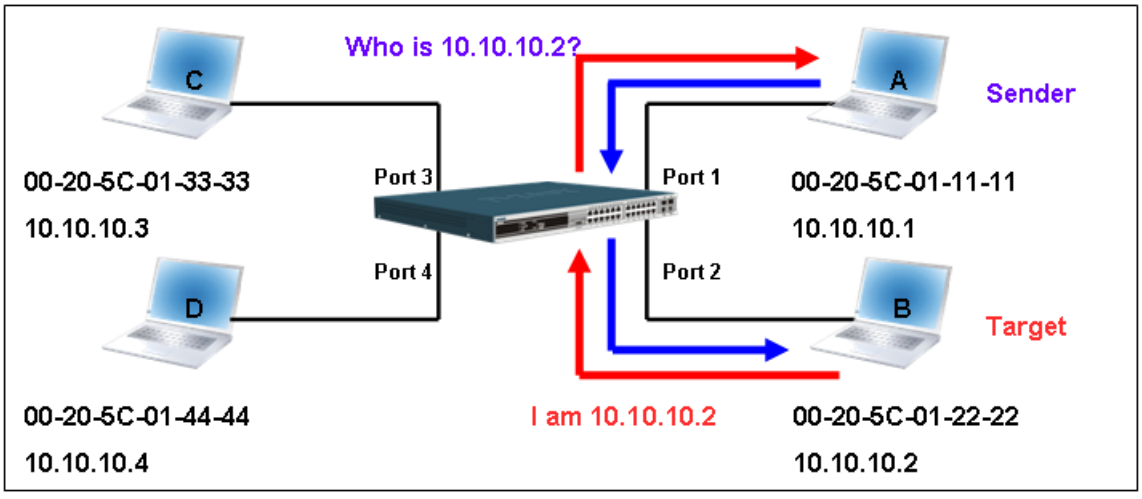


Figure-3

When PC B replies to the ARP request, its MAC address will be written into “Target H/W Address” in the ARP payload shown in Table-3. The ARP reply will be then encapsulated into the Ethernet frame again and sent back to the sender. The ARP reply is in a form of Unicast communication.

H/W type	Protocol type	H/W address length	Protocol address length	Operation	Sender H/W address	Sender protocol address	Target H/W address	Target protocol address
				ARP reply	00-20-5C-01-11-11	10.10.10.1	00-20-5C-01-22-22	10.10.10.2

Table – 3 (ARP Payload)

When PC B replies the query, the “Destination Address” in the Ethernet frame will be changed to PC A’s MAC address. The “Source Address” will be changed to PC B’s MAC address (see Table-4).

Destination address	Source address	Ether-type	ARP	FCS
00-20-5C-01-11-11	00-20-5C-01-22-22			

Table – 4 (Ethernet frame format)

The switch will also examine the “Source Address” of the Ethernet frame and find that the address is not in the Forwarding Table. The switch will learn PC B’s MAC and update its Forwarding Table.

Forwarding Table

Port1 00-20-5C-01-11-11
Port2 00-20-5C-01-22-22

How ARP spoofing attacks a network

ARP spoofing, also known as ARP poisoning, is a method to attack an Ethernet network which may allow an attacker to sniff data frames on a LAN, modify the traffic, or stop the traffic altogether (known as a Denial of Service - DoS attack). The principle of ARP spoofing is to send the fake, or spoofed ARP messages to an Ethernet network. Generally, the aim is to associate the attacker's or random MAC address with the IP address of another node (such as the default gateway). Any traffic meant for that IP address would be mistakenly re-directed to the node specified by the attacker.

IP spoofing attack is caused by Gratuitous ARP that occurs when a host sends an ARP request to resolve its own IP address. Figure-4 shows a hacker within a LAN to initiate ARP spoofing attack.

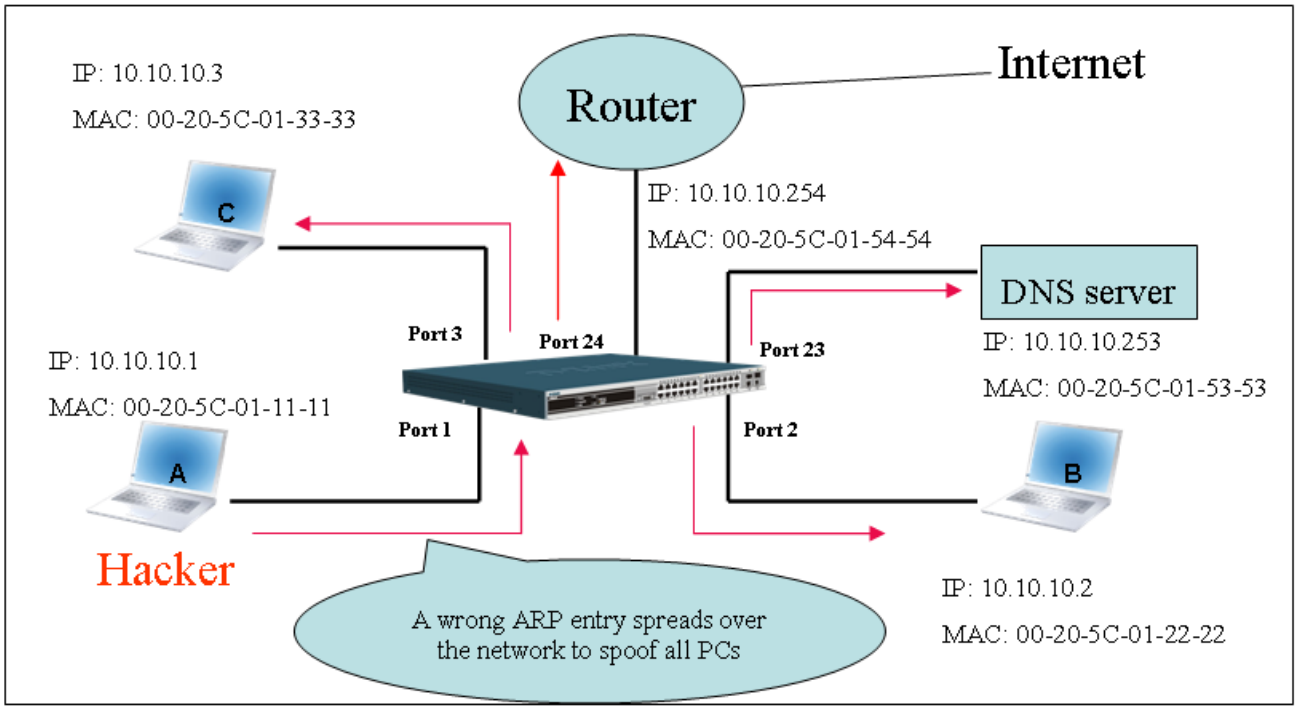


Figure-4

In the Gratuitous ARP packet, the “Sender protocol address” and “Target protocol address” are filled with the same source IP address. The “Sender H/W Address” and “Target H/W address” are filled with the same source MAC address. The destination MAC address is the Ethernet broadcast address (FF-FF-FF-FF-FF-FF). All nodes within the network will immediately update their own ARP table in accordance with the sender’s MAC and IP address. The format of Gratuitous ARP is shown in Table-5.

Ethernet			Gratuitous ARP								
Destination address	**Source address**	**Ethernet type**	**H/W type**	**Protocol type**	**H/W address length**	**Protocol address length**	**Operation**	**Sender H/W address**	**Sender protocol address**	**Target H/W address**	**Target protocol address**
(6-byte)	(6-byte)	(2-byte)	(2-byte)	(2-byte)	(1-byte)	(1-byte)	(2-byte)	(6-byte)	(4-byte)	(6-byte)	(4-byte)
FF-FF-FF-FF-FF-FF	00-20-5C-01-11-11	806					ARP reply	***00-20-5C-01-11-11***	***10.10.10.254***	***00-20-5C-01-11-11***	***10.10.10.254***

Table-5

A common DoS attack today can be done by associating a nonexistent or specified MAC address to the IP address of the network's default gateway. The malicious attacker only needs to broadcast ONE Gratuitous ARP to the network claiming it is the gateway so that the whole network operation will be turned down as all packets to the Internet will be directed to the wrong node.

Likewise, the attacker can either choose to forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it (man-in-the-middle attack). The hacker cheats the victim's PC to think that it is a router and cheats the router to think it is the victim. As can be seen in Figure-5 all traffic will be then sniffed by the hacker but the users will not notice anything happening.

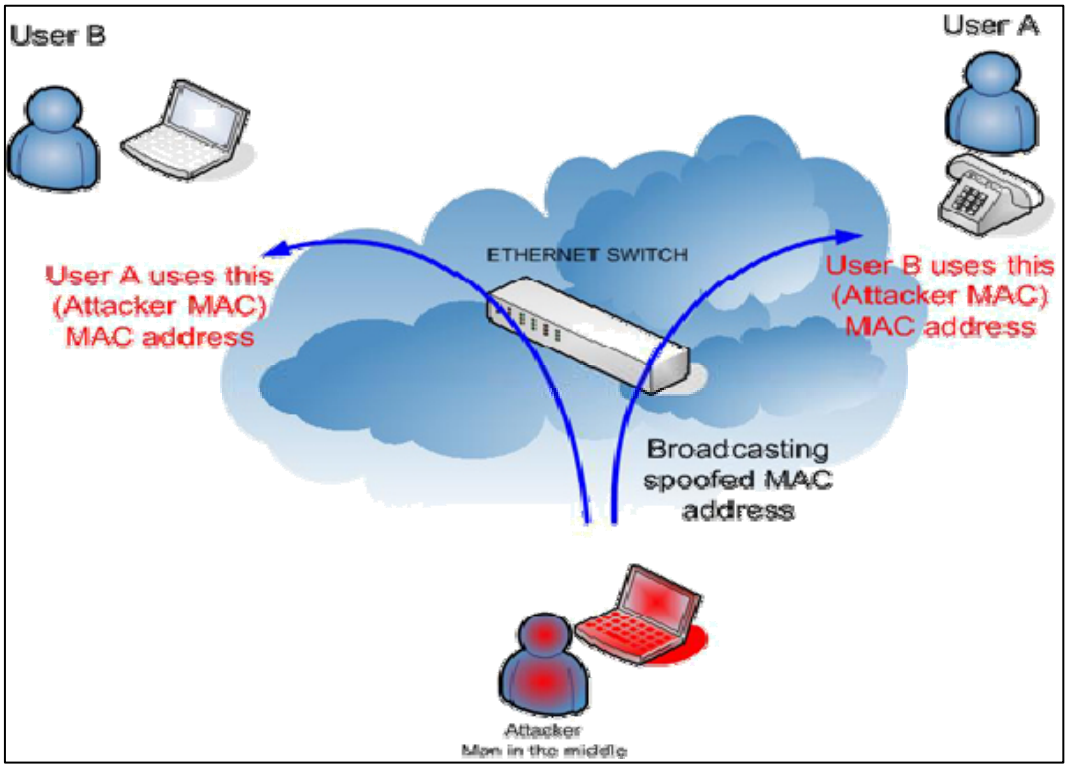
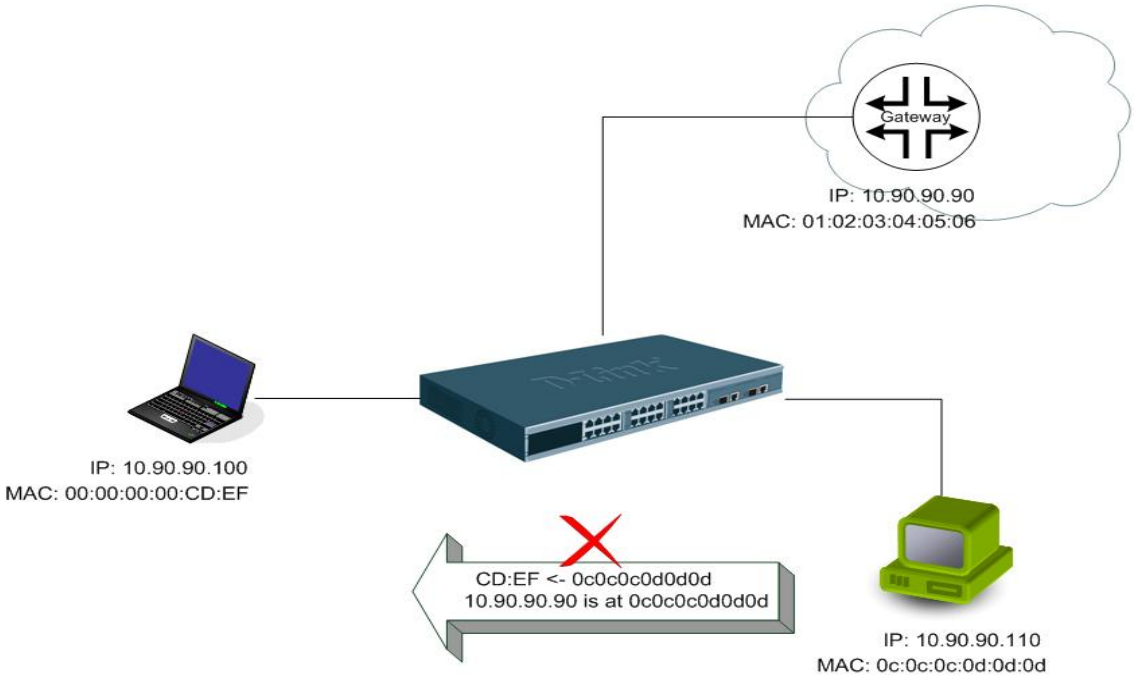


Figure-5

- **Prevent ARP spoofing via packet content ACL**

Concerning the common DoS attack today caused by the ARP spoofing, D-Link managed switch can effectively mitigate it via its unique Packet Content ACL.

For that reason the basic ACL can only filter ARP packets based on packet type, VLAN ID, Source and Destination MAC information, there is a need for further inspections of ARP packets. To prevent ARP spoofing attack, we will demonstrate here using Packet Content ACL on Switch to block the invalid ARP packets which contain fake gateway's MAC and IP binding.



Example topology

Configuration:

The configuration logic is listed below:

1. Only when the ARP matches the Source MAC address in Ethernet, the Sender MAC address and Sender IP address in the ARP protocol can pass through the switch. (In this example, it is the gateway's ARP.)
2. The switch will deny all other ARP packets which claim they are from the gateway's IP.

The design of Packet Content ACL on DES-3528/DES-3552 Switch Series enables users to inspect any offset_chunk. An offset_chunk is a 4-byte block in a HEX format which is utilized to match the individual field in an Ethernet frame. Each profile is allowed to contain up to a maximum of 4 offset_chunks. Furthermore, only one single profile of Packet Content ACL can be supported per switch. In other words, up to 16 bytes of total offset_chunks can be applied to each profile and a switch. Therefore, careful consideration is needed for planning the configuration of the valuable offset_chunks.

In Table-6, you will notice that the Offset_Chunk0 starts from 127 and ends at the 2nd byte. It can also be found that the offset_chunk is scratched from **1** but not zero.

Offset Chunk	Offset Chunk0	Offset Chunk1	Offset Chunk2	Offset Chunk3	Offset Chunk4	Offset Chunk5	Offset Chunk6	Offset Chunk7	Offset Chunk8	Offset Chunk9	Offset Chunk10	Offset Chunk11	Offset Chunk12	Offset Chunk13	Offset Chunk14	Offset Chunk15
Byte	127	3	7	11	15	19	23	27	31	35	39	43	47	51	55	59
Byte	128	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
Byte	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
Byte	2	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62

Offset Chunk	Offset Chunk15	Offset Chunk16	Offset Chunk17	Offset Chunk18	Offset Chunk19	Offset Chunk20	Offset Chunk21	Offset Chunk22	Offset Chunk23	Offset Chunk24	Offset Chunk25	Offset Chunk26	Offset Chunk27	Offset Chunk28	Offset Chunk129	Offset Chunk30
Byte	63	67	71	75	79	83	87	91	95	99	103	107	111	115	119	123
Byte	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124
Byte	65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125
Byte	66	70	74	78	82	86	90	94	98	102	106	110	114	118	122	126

Table-6: Chunk and Packet offset Indicates a completed ARP packet contained in the Ethernet frame, which is the pattern for the calculation of packet offset.

Ethernet **ARP**

Destination address	**Source address**	**Ethernet type**	**H/W type**	**Protocol type**	**H/W address length**	**Protocol address length**	**Operation**	**Sender H/W address**	**Sender protocol address**	**Target H/W address**	**Target protocol address**
(6-byte)	(6-byte)	(2-byte)	(2-byte)	(2-byte)	(1-byte)	(1-byte)	(2-byte)	(6-byte)	(4-byte)	(6-byte)	(4-byte)
	01 02 03 04 05 06	0806							0a5a5a5a (10.90.90.90)		

Table-7: A completed ARP packet contained in Ethernet frame

	Command	Description
Step1	create access_profile profile_id 1 ethernet source_mac FF-FF-FF-FF-FF-FF ethernet_type	- Create access profile 1 To match Ethernet Type and Source MAC address.
Step2	config access_profile profile_id 1 add access_id 1 ethernet source_mac 01-02-03-04-05-06 ethernet_type 0x806 port 1-27 permit	- Configure access profile 1 - Only if the gateway's ARP packet that contains the correct Source MAC in Ethernet frame can pass through the switch.
Step3	create access_profile profile_id 2 packet_content_mask offset_chunk_1 3 0x0000FFFF Ethernet Type(2-byte) offset_chunk_2 7 0x0000FFFF Sdr IP(First 2-byte) offset_chunk_3 8 0xFFFF0000 Sdr IP(Last 2-byte)	- Create access profile 2 - The first Chunk starts from Chunk 3: mask for Ethernet Type (Blue in Table-6: 13th & 14th bytes) - The second Chunk starts from Chunk 7: mask for Sender IP (First 2-byte) in ARP packet (Green in Table-6: 29th & 30th bytes) - The third Chunk starts from Chunk 8: mask for Sender IP (Last 2-byte) in ARP packet (Brown in Table-6: 31st & 32nd bytes)
Step4	config access_profile profile_id 2 add access_id 1 packet_content offset_chunk_1 0x00000806 Ethernet Type(2-byte): ARP offset_chunk_2 0x00000A5A Sdr IP(First 2-byte): 10.90 offset_chunk_3 0x5A5A0000 Sdr IP(Last 2-byte): 90.90 port 1-27 deny	- Configure access profile 2 - The rest ARP packets whose Sender IP claim they are the gateway's IP will be dropped.
Step5	Save	- Save config

Appendix B

System Log Entries

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this Switch.

Category	Event Description	Log Information	Severity
system	System warm start	[Uint <unitID>,] System warm start	Critical
	System cold start	[Uint <unitID>,] System cold start	Critical
	Configuration saved to flash	[Unit <unitID>,] Configuration saved to flash (Username: <username>)	Informational
	System log saved to flash	[Unit <unitID>,] System log saved to flash (Username: <username>)	Informational
	Configuration and log saved to flash	[Unit <unitID>,] Configuration and log saved to flash(Username: <username>)	Informational
	Internal Power failed	[Unit <unitID>,] Internal Power failed	Critical
	Internal Power is recovered	[Unit <unitID>,] Internal Power is recovered	Critical
	Redundant Power failed	[Unit <unitID>,] Redundant Power failed	Critical
	Redundant Power is working	[Unit <unitID>,] Redundant Power is working	Critical
	Access flash failed	[Unit <unitID>,] Access flash failed (operation: <operation>, physical address: <address>)	Warning
	Temperatrue sensor alarms	[Unit <unitID>,] Temperatrue sensor <sensorID> enters alarm state(threshold: <temperature>)	Warning
	Temperatrue sensor recoveries	[Unit <unitID>,] Temperatrue sensor <sensorID> enters normal state(threshold: <temperature>)	Informational
up/down-load	Firmware upgraded successfully	[Unit <unitID>,] Firmware upgraded by console successfully (Username: <username>)	Informational
	Firmware upgrade was unsuccessful	[Unit <unitID>,] Firmware upgrade by console was unsuccessful! (Username: <username>)	Warning
	Configuration successfully downloaded	Configuration successfully downloaded by console(Username: <username>)	Informational
	Configuration download was unsuccessful	Configuration download by console was unsuccessful! (Username: <username>)	Warning
	Configuration successfully uploaded	Configuration successfully uploaded by console (Username: <username>)	Informational
	Configuration upload was	Configuration upload by console was unsuccessful!	Warning

	unsuccessful	(Username: <username>)	
	Log message successfully uploaded	Log message successfully uploaded by console (Username: <username>)	Informational
	Log message upload was unsuccessful	Log message upload by console was unsuccessful! (Username: <username>)	Warning
Interface	Port link up	Port <unitID:portNum> link up, <link state>	Informational
	Port link down	Port <unitID:portNum> link down	Informational
Console	Successful login through Console	[Uint <unitID>,] Successful login through Console (Username: <username>)	Informational
	Login failed through Console	[Uint <unitID>,] Login failed through Console (Username: <username>)	Warning
	Logout through Console	[Uint <unitID>,] Logout through Console (Username: <username>)	Informational
	Console session timed out	[Uint <unitID>,] Console session timed out (Username: <username>)	Informational
Web	Successful login through Web	Successful login through Web (Username: <username>, IP: <ipaddr>)	Informational
	Login failed through Web	Login failed through Web (Username: <username>, IP: <ipaddr>)	Warning
	Logout through Web	Logout through Web (Username: <username>, IP: <ipaddr>)	Informational
SSL	Successful login through Web(SSL)	Successful login through Web(SSL) (Username: <username>, IP: <ipaddr>)	Informational
	Login failed through Web(SSL)	Login failed through Web(SSL) (Username: <username>, IP: <ipaddr>)	Warning
	Logout through Web(SSL)	Logout through Web(SSL) (Username: <username>, IP: <ipaddr>)	Informational
	Web(SSL) session timed out	Web(SSL) session timed out (Username: <username>, IP: <ipaddr>)	Informational
Telnet	Successful login through Telnet	Successful login through Telnet (Username: <username>, IP: <ipaddr>)	Informational
	Login failed through Telnet	Login failed through Telnet (Username: <username>, IP: <ipaddr>)	Warning
	Logout through Telnet	Logout through Telnet (Username: <username>, IP: <ipaddr>)	Informational
	Telnet session timed out	Telnet session timed out (Username: <username>, IP: <ipaddr>)	Informational
SNMP	SNMP request received with invalid community string	SNMP request received from <ipAddress> with invalid community string!	Informational

STP	Topology changed	Topology changed	Informational
	New Root selected	New Root selected	Informational
	BPDU Loop Back on port	BPDU Loop Back on Port <unitID:portNum>	Warning
	Spanning Tree Protocol is enabled	Spanning Tree Protocol is enabled	Informational
	Spanning Tree Protocol is disabled	Spanning Tree Protocol is disabled	Informational
SSH	Successful login through SSH	Successful login through SSH (Username: <username>, IP: <ipaddr>)	Informational
	Login failed through SSH	Login failed through SSH (Username: <username>, IP: <ipaddr>)	Warning
	Logout through SSH	Logout through SSH (Username: <username>, IP: <ipaddr>)	Informational
	SSH session timed out	SSH session timed out (Username: <username>, IP: <ipaddr>)	Informational
	SSH server is enabled	SSH server is enabled	Informational
	SSH server is disabled	SSH server is disabled	Informational
AAA	Authentication Policy is enabled	Authentication Policy is enabled (Module: AAA)	Informational
	Authentication Policy is disabled	Authentication Policy is disabled (Module: AAA)	Informational
	Successful login through Console authenticated by AAA local method	Successful login through Console authenticated by AAA local method (Username: <username>)	Informational
	Login failed through Console authenticated by AAA local method	Login failed through Console authenticated by AAA local method (Username: <username>)	Warning
	Successful login through Web authenticated by AAA local method	Successful login through Web from <userIP> authenticated by AAA local method (Username: <username>)	Informational
	Login failed through Web authenticated by AAA local method	Login failed failed through Web from <userIP> authenticated by AAA local method (Username: <username>)	Warning
	Successful login through Web(SSL) authenticated by AAA local method	Successful login through Web(SSL) from <userIP> authenticated by AAA local method (Username: <username>)	Informational
	Login failed through Web(SSL) authenticated by AAA local method	Login failed through Web(SSL) from <userIP> authenticated by AAA local method (Username: <username>)	Warning

	Successful login through Telnet authenticated by AAA local method	Successful login through Telnet from <userIP> authenticated by AAA local method (Username: <username>)	Informational
	Login failed through Telnet authenticated by AAA local method	Login failed through Telnet from <userIP> authenticated by AAA local method (Username: <username>)	Warning
	Successful login through SSH authenticated by AAA local method	Successful login through SSH from <userIP> authenticated by AAA local method (Username: <username>)	Informational
	Login failed through SSH authenticated by AAA local method	Login failed through SSH from <userIP> authenticated by AAA local method (Username: <username>)	Warning
	Successful login through Console authenticated by AAA none method	Successful login through Console authenticated by AAA none method (Username: <username>)	Informational
	Successful login through Web authenticated by AAA none method	Successful login through Web from <userIP> authenticated by AAA none method (Username: <username>)	Informational
	Successful login through Web(SSL) authenticated by AAA none method	Successful login through Web(SSL) from <userIP> authenticated by AAA none method (Username: <username>)	Informational
	Successful login through Telnet authenticated by AAA none method	Successful login through Telnet from <userIP> authenticated by AAA none method (Username: <username>)	Informational
	Successful login through SSH authenticated by AAA none method	Successful login through SSH from <userIP> authenticated by AAA none method (Username: <username>)	Informational
	Successful login through Console authenticated by AAA server	Successful login through Console authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Login failed through Console authenticated by AAA server	Login failed through Console authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Successful login through Web authenticated by AAA server	Successful login through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Login failed through Web authenticated by AAA server	Login failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Successful login through Web(SSL) authenticated by AAA server	Successful login through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Login failed through Web(SSL) authenticated by AAA server	Login failed through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning

	Login failed through Web(SSL) due to AAA server timeout or improper configuration	Login failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Successful login through Telnet authenticated by AAA server	Successful login through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Login failed through Telnet authenticated by AAA server	Login failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Successful login through SSH authenticated by AAA server	Successful login through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Login failed through SSH authenticated by AAA server	Login failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Successful Enable Admin through Console authenticated by AAA local_enable method	Successful Enable Admin through Console authenticated by AAA local_enable method (Username: <username>)	Informational
	Enable Admin failed through Console authenticated by AAA local_enable method	Enable Admin failed through Console authenticated by AAA local_enable method (Username: <username>)	Warning
	Successful Enable Admin through Web authenticated by AAA local_enable method	Successful Enable Admin through Web from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational
	Enable Admin failed through Web authenticated by AAA local_enable method	Enable Admin failed through Web from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning
	Successful Enable Admin through Telnet authenticated by AAA local_enable method	Successful Enable Admin through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational
	Enable Admin failed through Telnet authenticated by AAA local_enable method	Enable Admin failed through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning
	Successful Enable Admin through SSH authenticated by AAA local_enable method	Successful Enable Admin through SSH from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational
	Enable Admin failed through SSH authenticated by AAA local_enable method	Enable Admin failed through SSH from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning

	Successful Enable Admin through Console authenticated by AAA none method	Successful Enable Admin through Console authenticated by AAA none method (Username: <username>)	Informational
	Successful Enable Admin through Web authenticated by AAA none method	Successful Enable Admin through Web from <userIP> authenticated by AAA none method (Username: <username>)	Informational
	Successful Enable Admin through Telnet authenticated by AAA none method	Successful Enable Admin through Telnet from <userIP> authenticated by AAA none method (Username: <username>)	Informational
	Successful Enable Admin through SSH authenticated by AAA none method	Successful Enable Admin through SSH from <userIP> authenticated by AAA none method (Username: <username>)	Informational
	Successful Enable Admin through Console authenticated by AAA server	Successful Enable Admin through Console authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Enable Admin failed through Console authenticated by AAA server	Enable Admin failed through Console authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Successful Enable Admin through Web authenticated by AAA server	Successful Enable Admin through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Enable Admin failed through Web authenticated by AAA server	Enable Admin failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Successful Enable Admin through Telnet authenticated by AAA server	Successful Enable Admin through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Enable Admin failed through Telnet authenticated by AAA server	Enable Admin failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Successful Enable Admin through SSH authenticated by AAA server	Successful Enable Admin through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Enable Admin failed through SSH authenticated by AAA server	Enable Admin failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Login failed through Console due to AAA server timeout or improper configuration.	Login failed through Console due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Enable Admin failed through Console due to AAA server timeout or	Enable Admin failed through Console due to AAA server timeout or improper configuration (Username:	Warning

	improper configuration.	<username>)	
	Login failed through Web from user due to AAA server timeout or improper configuration.	Login failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Enable Admin failed through Web from user due to AAA server timeout or improper configuration.	Enable Admin failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Login failed through Web(SSL) from user due to AAA server timeout or improper configuration	Login failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Enable Admin failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration.	Enable Admin failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Login failed through Telnet from user due to AAA server timeout or improper configuration.	Login failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Enable Admin failed through Telnet from user due to AAA server timeout or improper configuration.	Enable Admin failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Login failed through SSH from user due to AAA server timeout or improper configuration.	Login failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Enable Admin failed through SSH from user due to AAA server timeout or improper configuration.	Enable Admin failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	AAA server response is wrong	AAA server <serverIP> (Protocol: <protocol>) response is wron	Warning
	AAA doesn't support this functionality	AAA doesn't support this functionality	Informational
Port security	Port security has exceeded its maximum learning size and will not learn any new addresses	Port security violation mac addrss <macaddr> on locking address full port <unitID:portNum>	Warning
Safeguard Engine	Safeguard Engine is in normal mode	Safeguard Engine enters NORMAL mode	Informational
	Safeguard Engine is in filtering packet mode	Safeguard Engine enters EXHAUSTED mode	Warning
Packet Storm	Broadcast strom occurrence	Port <portNum> Broadcast storm is occurring	Warning

	Broadcast storm cleared	Port <portNum> Broadcast storm has cleared	Informational
	Multicast storm occurrence	Port <portNum> Multicast storm is occurring	Warning
	Multicast storm cleared	Port <portNum> Multicast storm has cleared	Informational
	Port shut down due to a packet storm	Port <portNum> is currently shut down due to a packet storm	Warning
IP-MAC-PORT Binding	Unauthenticated ip address and discard by ip mac port binding	Unauthenticated IP-MAC address and discarded by ip mac port binding (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)	Warning
	Unauthenticated IP address encountered and discarded by ip IP-MAC port binding	Unauthenticated IP-MAC address and discarded by IP-MAC port binding (IP: <ipaddr>, MAC: <macaddr>, Port: <portNum>)	Warning
	Dynamic IMPB entry is conflict with static ARP	Dynamic IMPB entry is conflict with static ARP(IP: <ipaddr>, MAC: <macaddr>, Port: <[unitID:]portNum>)	Informational
	Dynamic IMPB entry conflicts with static IMPB	Dynamic IMPB entry conflicts with static IMPB: IP: <ipaddr>, MAC: <macaddr>, Port: <[unitID:]portNum>	Informational
	Dynamic IMPB entry cannot be created	Creating IMPB entry Failed due to no ACL rule available: IP: <ipaddr>, MAC: <macaddr>, Port: <[unitID:]portNum>	Informational
	Port enter IMPB block state	Port <[unitID:]portNum> enter IMPB block state	Informational
	Port recover from IMPB block state	Port <[unitID:]portNum> recover from IMPB block state	Informational
LBD	LBD loop occurred	Port <portNum> LBD loop occurred. Port blocked	Critical
	LBD port recovered. Loop detection restarted	Port <portNum> LBD port recovered. Loop detection restarted	Informational
	LBD loop occurred. Packet discard begun	Port <portNum> VID <vid> LBD loop occurred. Packet discard begun	Critical
	LBD recovered. Loop detection restarted	Port <portNum> VID <vid> LBD recovered. Loop detection restarted	Informational
	Loop vlan number overflow,	Loop vlan number overflow	Informational
DOS	Spoofing attack	Possible spoofing attack from IP <ipaddr> MAC <macaddr> port <[unitID:]portNum>	Critical
JWAC	A user fails to pass the authentication	JWAC unauthenticated user (Username: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <[unitID:]portNum>)	Warning
	system stop learning	JWAC enters stop learning state.	Warning
	system recover learning	JWAC recovers from stop learning state.	Warning
WAC	A user fails to pass the authentication	WAC unauthenticated user (Username: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <[unitID:]portNum>)	Warning
	system stop learning	WAC enters stop learning state.	Warning

	system recover learning	WAC recovers from stop learning state.	Warning
MAC	Login OK	MAC-AC login successful (MAC: <macaddr>, Port: <[unitID:]portNum>, VID: <vid>)	Information
	Login fail	MAC-AC login rejected (MAC: <macaddr>, Port: <[unitID:]portNum>, VID: <vid>)	Warning
	Logout normal	MAC-AC host aged out (MAC: <macaddr>, Port: <[unitID:]portNum>, VID: <vid>)	Information
IP and Password Changed	IP Address change activity	Unit <unitID>,Management IP address was changed by (Username: <username>,IP:<ipaddr>)	Informational
	Password change activity	Unit <unitID>,Password was changed by (Username: <username>,IP:<ipaddr>)	Informational
Gratuitous ARP	Conflict IP was detected with this device	Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>, Interface: <ipif_name>)	Informational
CFM	CFM remote detects a defect	CFM remote detects a defect. MD Level:<level>, VLAN:<vid>, Local(Port <portNum>, Direction:<direcrtion>)	Informational
	CFM remote MAC error	CFM remote MAC error. MD Level:<level>, VLAN:<vid>, Local(Port <portNum>, Direction:<direcrtion>)	Warning
	CFM remote down	CFM remote down. MD Level:<level>, VLAN:<vid>, Local(Port %S, Direction:<direcrtion>)	Warning
	CFM error ccm	CFM error ccm. MD Level:<level>, VLAN:<vid>, Local(Port <portNum>, Direction:<direcrtion>) Remote(MEPID:<mepid>,MAC:<macaddr>)	Warning
	CFM cross-connect	CFM cross-connect. VLAN:<vid>, Local(MD Level:<level>, Port <portNum>, Direction:<direcrtion>) Remote(MEPID:<mepid>,MAC:<macaddr>)	Critical
Stacking	Hot insert	Unit <unitID>, MAC:<macaddr> Hot insert	Informational
	Hot remove	Unit <unitID>, MAC:<macaddr> Hot remove	Informational
	Firmware upgraded to SLAVE successfully	Firmware upgraded to SLAVE by console successfully (Username: <username>)	Informational
	Firmware upgraded to SLAVE unsuccessfully	Firmware upgraded to SLAVE by console unsuccessfully! (Username: <username>)	Warning
	Stacking topology change.	Stacking topology is <Stack_TP_TYPE>. Master(Unit <unitID>, MAC:<macaddr>).	Informational
	box id conflict	Unit <unitID> Conflict	Informational
BPDU Protection	Port enter BPDU under attacking state	Port <[unitID:] portNum> enter BPDU under attacking state (mode: <mode>)	Informational
	Port recover from BPDU under attacking state manually	Port <[unitID:] portNum> recover from BPDU under attacking state manually	Informational

	Port recover from BPDU under attacking state automatically	Port <[unitID:] portNum> recover from BPDU under attacking state automatically	Informational
DHCP	Detect untrusted DHCP server IP address	Detected untrusted DHCP server(IP: <ipaddr>, Port: <[unitID:]portNum>)	Informational
Voice VLAN	New voice device detected	New voice device detected :<macaddr>, Trunk:<trunk_ID>	Informational
	Trunk add into voice VLAN	Trunk <trunk_ID> add into voice VLAN <vid>	Informational
	Trunk remove from voice VLAN	Trunk <trunk_ID> remove from voice VLAN <vid>	Informational

DES-3200-10/18/28/28F Trap List

Trap Name/OID	Variable Bind	Format	MIB Name	Severity
coldStart 1.3.6.1.6.3.1.1.5.1	None	V2	RFC1907 (SNMPv2-MIB)	Critical
warmStart 1.3.6.1.6.3.1.1.5.2	None	V2	RFC1907 (SNMPv2-MIB)	Critical
authenticationFailure 1.3.6.1.6.3.1.1.5.5	None	V2	RFC1907 (SNMPv2-MIB)	Informational
linkDown 1.3.6.1.6.3.1.1.5.3	ifIndex, ifAdminStatus, ifOperStatus	V2	RFC2863 (IF-MIB)	Informational
linkup 1.3.6.1.6.3.1.1.5.4	ifIndex, ifAdminStatus, ifOperStatus	V2	RFC2863 (IF-MIB)	Informational
newRoot 1.3.6.1.2.1.17.0.1	None	V2	RFC1493 (BRIDGE-MIB)	Informational
topologyChange 1.3.6.1.2.1.17.0.2	None	V2	RFC1493 (BRIDGE-MIB)	Informational

Proprietary Trap List

Trap Name/OID	Variable Bind	Format	MIB Name	Severity
swL2macNotification 1.3.6.1.4.1.171.11.113.1.1.2.20.0.2 1.3.6.1.4.1.171.11.113.1.2.2.20.0.2 1.3.6.1.4.1.171.11.113.1.1.3.20.0.2 1.3.6.1.4.1.171.11.113.1.1.4.20.0.2	swL2macNotifyInfo	V2	L2Mgmt-MIB	Warning
SwIpMacBindingViolationTrap 1.3.6.1.4.1.171.12.23.5.0.1	swIpMacBindingPortIndex swIpMacBindingViolationIP swIpMacBindingViolationMac	V2	IPMacBind-MIB	Warning
swIpMacBindingStopLearningTrap	swIpMacBindingPortIndex	V2	IPMacBind-MIB	Warning

1.3.6.1.4.1.171.12.23.5.0.2				
swIpMacBindingRecoverLearningTrap 1.3.6.1.4.1.171.12.23.5.0.3	swIpMacBindingPortIndex	V2	IPMacBind-MIB	Warning
swMacBasedAuthLoggedSuccess 1.3.6.1.4.1.171.12.35.11.1.0.1	swMacBasedAuthInfoMacIndex swMacBasedAuthInfoPortIndex swMacBasedAuthVID	V2	MBA-MIB	Warning
SwMacBasedAuthLoggedFail 1.3.6.1.4.1.171.12.35.11.1.0.2	swMacBasedAuthInfoMacIndex swMacBasedAuthInfoPortIndex swMacBasedAuthVID	V2	MBA-MIB	Warning
SwMacBasedAuthAgesOut 1.3.6.1.4.1.171.12.35.11.1.0.3	swMacBasedAuthInfoMacIndex swMacBasedAuthInfoPortIndex swMacBasedAuthVID	V2	MBA-MIB	Warning
swPktStormOccurred 1.3.6.1.4.1.171.12.25.5.0.1	swPktStormCtrlPortIndex	V2	PktStormCtrl-MIB	Warning
swPktStormCleared 1.3.6.1.4.1.171.12.25.5.0.2	swPktStormCtrlPortIndex	V2	PktStormCtrl-MIB	Warning
agentGratuitousARPTrap 1.3.6.1.4.1.171.12.1.7.2.0.5	agentGratuitousARPIpAddr agentGratuitousARPMacAddr agentGratuitousARPPortNumber agentGratuitousARPInterfaceName	V2	Genmgmt-MIB	Warning
swSafeGuardChgToExhausted 1.3.6.1.4.1.171.12.19.4.1.0.1	swSafeGuardCurrentStatus	V2	SafeGuard Engine-MIB	Warning
swSafeGuardChgToNormal 1.3.6.1.4.1.171.12.19.4.1.0.2	swSafeGuardCurrentStatus	V2	SafeGuard Engine-MIB	Warning
swDoSAttackDetected 1.3.6.1.4.1.171.12.59.4.0.1	swDoSCtrlType swDoSNotifyVarIpAddr swDoSNotifyVarPortNumber	V2	DoSPrev-MIB	Warning
swL2PortSecurityViolationTrap 1.3.6.1.4.1.171.11.113.1.1.2.20.0.1 1.3.6.1.4.1.171.11.113.1.2.2.20.0.1 1.3.6.1.4.1.171.11.113.1.3.2.20.0.1 1.3.6.1.4.1.171.11.113.1.4.2.20.0.1	swL2PortSecurityPortIndex swL2PortSecurityViolationMac	V2	L2mgmt-MIB	Warning

Appendix C

Glossary

1000BASE-SX: A short laser wavelength on multimode fiber optic cable for a maximum length of 2000 meters

1000BASE-LX: A long wavelength for a "long haul" fiber optic cable for a maximum length of 10 kilometers

1000BASE-T: 1000Mbps Ethernet implementation over Category 5E cable.

100BASE-FX: 100Mbps Ethernet implementation over fiber.

100BASE-TX: 100Mbps Ethernet implementation over Category 5 and Type 1 Twisted Pair cabling.

10BASE-T: The IEEE 802.3 specification for Ethernet over Unshielded Twisted Pair (UTP) cabling.

aging: The automatic removal of dynamic entries from the Switch Database which have timed-out and are no longer valid.

ATM: Asynchronous Transfer Mode. A connection oriented transmission protocol based on fixed length cells (packets). ATM is designed to carry a complete range of user traffic, including voice, data and video signals.

auto-negotiation: A feature on a port, which allows it to advertise its capabilities for speed, duplex and flow control. When connected to an end station that also supports auto-negotiation, the link can self-detect its optimum operating setup.

backbone port: A port which does not learn device addresses, and which receives all frames with an unknown address. Backbone ports are normally used to connect the Switch to the backbone of your network. Note that backbone ports were formerly known as designated downlink ports.

backbone: The part of a network used as the primary path for transporting traffic between network segments.

bandwidth: Information capacity, measured in bits per second that a channel can transmit. The bandwidth of Ethernet is 10Mbps, the bandwidth of Fast Ethernet is 100Mbps.

baud rate: The switching speed of a line. Also known as line speed between network segments.

BOOTP: The BOOTP protocol allows you to automatically map an IP address to a given MAC address each time a device is started. In addition, the protocol can assign the subnet mask and default gateway to a device.

bridge: A device that interconnects local or remote networks no matter what higher-level protocols are involved. Bridges form a single logical network, centralizing network administration.

broadcast: A message sent to all destination devices on the network.

broadcast storm: Multiple simultaneous broadcasts that typically absorb available network bandwidth and can cause network failure.

console port: The port on the Switch accepting a terminal or modem connector. It changes the parallel arrangement of data within computers to the serial form used on data transmission links. This port is most often used for dedicated local management.

CSMA/CD: Channel access method used by Ethernet and IEEE 802.3 standards in which devices transmit only after finding the data channel clear for some period of time. When two devices transmit simultaneously, a collision occurs and the colliding devices delay their retransmissions for a random amount of time.

data center switching: The point of aggregation within a corporate network where a switch provides high-performance access to server farms, a high-speed backbone connection and a control point for network management and security.

Ethernet: A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks operate at 10Mbps using CSMA/CD to run over cabling.

Fast Ethernet: 100Mbps technology based on the Ethernet/CMSA/CD network access method.

Flow Control: (IEEE 802.3z) A means of holding packets back at the transmit port of the connected end station. Prevents packet loss at a congested switch port.

forwarding: The process of sending a packet toward its destination by an internetworking device.

full duplex: A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.

half duplex: A system that allows packets to be transmitted and received, but not at the same time. Contrast with full duplex.

IP address: Internet Protocol address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with full-stops (periods), and is made up of a network section, an optional subnet section and a host section.

IPX: Internetwork Packet Exchange. A protocol allowing communication in a NetWare network.

LAN - Local Area Network: A network of connected computing resources (such as PCs, printers, servers) covering a relatively small geographic area (usually not larger than a floor or building). Characterized by high data rates and low error rates.

latency: The delay between the time a device receives a packet and the time the packet is forwarded out of the destination port.

line speed: See baud rate.

main port: The port in a resilient link that carries data traffic in normal operating conditions.

MDI - Medium Dependent Interface: An Ethernet port connection where the transmitter of one device is connected to the receiver of another device.

MDI-X - Medium Dependent Interface Cross-over: An Ethernet port connection where the internal transmit and receive lines are crossed.

MIB - Management Information Base: Stores a device's management characteristics and parameters. MIBs are used by the Simple Network Management Protocol (SNMP) to contain attributes of their managed systems. The Switch contains its own internal MIB.

multicast: Single packets copied to a specific subset of network addresses. These addresses are specified in the destination-address field of the packet.

protocol: A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.

resilient link: A pair of ports that can be configured so that one will take over data transmission should the other fail. See also main port and standby port.

RJ-45: Standard 8-wire connectors for IEEE 802.3 10BASE-T networks.

RMON: Remote Monitoring. A subset of SNMP MIB II that allows monitoring and management capabilities by addressing up to ten different groups of information.

RPS - Redundant Power System: A device that provides a backup source of power when connected to the Switch.

server farm: A cluster of servers in a centralized location serving a large user population.

SLIP - Serial Line Internet Protocol: A protocol, which allows IP to run over a serial line connection.

SNMP - Simple Network Management Protocol: A protocol originally designed to be used in managing TCP/IP internets. SNMP is presently implemented on a wide range of computers and networking equipment and may be used to manage many aspects of network and end station operation.

Spanning Tree Protocol (STP): A bridge-based system for providing fault tolerance on networks. STP works by allowing you to implement parallel paths for network traffic, and ensure that redundant paths are disabled when the main paths are operational and enabled if the main paths fail.

stack: A group of network devices that are integrated to form a single logical device.

standby port: The port in a resilient link that will take over data transmission if the main port in the link fails.

switch: A device, which filters, forwards and floods packets based on the packet's destination address. The switch learns the addresses associated with each switch port and builds tables based on this information to be used for the switching decision.

TCP/IP: A layered set of communications protocols providing Telnet terminal emulation, FTP file transfer, and other services for communication among a wide range of computer equipment.

Telnet: A TCP/IP application protocol that provides virtual terminal service, letting a user log in to another computer system and access a host as if the user were connected directly to the host.

TFTP - Trivial File Transfer Protocol: Allows you to transfer files (such as software upgrades) from a remote device using your switch's local management capabilities.

UDP - User Datagram Protocol: An Internet standard protocol that allows an application program on one device to send a datagram to an application program on another device.

VLAN - Virtual LAN: A group of location- and topology-independent devices that communicate as if they are on a common physical LAN.

VLT - Virtual LAN Trunk: A Switch-to-Switch link which carries traffic for all the VLANs on each Switch.

VT100: A type of terminal that uses ASCII characters. VT100 screens have a text-based appearance.